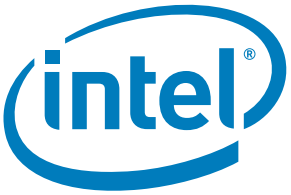


Intel® Xeon® Processor D-1500 Product Family

Datasheet - Volume 1 of 4: Integrated Platform Controller Hub

April 2021

Doc. No.: 332050-003

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Learn more at intel.com, or from the OEM or retailer.

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

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

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document. The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

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

Warning: Altering PC clock or memory frequency and/or voltage may (i) reduce system stability and use life of the system, memory and processor; (ii) cause the processor and other system components to fail; (iii) cause reductions in system performance; (iv) cause additional heat or other damage; and (v) affect system data integrity. Intel assumes no responsibility that the memory, included if used with altered clock frequencies and/or voltages, will be fit for any particular purpose. Check with memory manufacturer for warranty and additional details.

Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

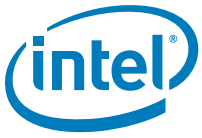
Intel® AMT should be used by a knowledgeable IT administrator and requires enabled systems, software, activation, and connection to a corporate network. Intel® AMT functionality on mobile systems may be limited in some situations. Your results will depend on your specific implementation. Learn more by visiting Intel® Active Management Technology.

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

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

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

Copyright © 2021, Intel Corporation. All Rights Reserved.

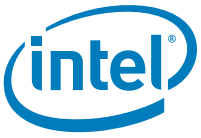


Content

1 Introduction 24
1.1 About This Manual 24
1.1.1 Chapter Descriptions 25
1.2 Overview 26
1.2.1 Capability Overview 27
1.3 Intel® Xeon® Processor D-1500 Product Family Integrated Chipset Definition 32
1.4 Device and Revision ID Table 32

2 Intel® Xeon® Processor D-1500 Product Family and System Clocks 35
2.1 Straps Related to Clock Configuration 35
2.2 SoC Clocking Requirements 35
2.3 Functional Blocks 37
2.4 Clock Configuration Access Overview 37
2.5 Integrated Clock Controller (ICC) Registers 38
2.5.1 ICC Registers under Intel® Management Engine (Intel® ME) Control 38

3 Functional Description 49
3.1 PCI-to-PCI Bridge 49
3.1.1 PCI Legacy Mode 49
3.2 PCI Express* Root Ports (D28:F0~F7) 49
3.2.1 Supported PCIe* Port Configurations 50
3.2.2 Interrupt Generation 50
3.2.3 Power Management 51
3.2.4 SERR# Generation 52
3.2.5 Hot-Plug 53
3.3 Gigabit Ethernet Controller (B0:D25:F0) 55
3.3.1 GbE PCI Express* Bus Interface 57
3.3.2 Error Events and Error Reporting 57
3.3.3 Ethernet Interface 58
3.3.4 PCI Power Management 58
3.3.5 Configurable LEDs 61
3.3.6 Function Level Reset Support (FLR) 61
3.4 Low Pin Count (LPC) Bridge (with System and Management Functions) (D31:F0) 62
3.4.1 LPC Interface 62
3.5 DMA Operation (D31:F0) 67
3.5.1 Channel Priority 68
3.5.2 Address Compatibility Mode 68
3.5.3 Summary of DMA Transfer Sizes 69
3.5.4 Autoinitialize 69
3.5.5 Software Commands 70
3.6 Low Pin Count (LPC) DMA 70
3.6.1 Asserting DMA Requests 70
3.6.2 Abandoning DMA Requests 71
3.6.3 General Flow of DMA Transfers 71
3.6.4 Terminal Count 72
3.6.5 Verify Mode 72
3.6.6 DMA Request De-assertion 72
3.6.7 SYNC Field / LDRQ# Rules 73
3.7 8254 Timers (D31:F0) 74
3.7.1 Timer Programming 74
3.7.2 Reading From the Interval Timer 75
3.8 8259 Programmable Interrupt Controllers (PIC) (D31:F0) 77
3.8.1 Interrupt Handling 78
3.8.2 Initialization Command Words (ICWx) 79
3.8.3 Operation Command Words (OCW) 80
3.8.4 Modes of Operation 80
3.8.5 Masking Interrupts 82
3.8.6 Steering PCI Interrupts 83
3.9 Advanced Programmable Interrupt Controller (APIC) (D31:F0) 83
3.9.1 Interrupt Handling 83
3.9.2 Interrupt Mapping 84
3.9.3 PCI / PCI Express* Message-Based Interrupts 85
3.9.4 IOxAPIC Address Remapping 85
3.9.5 External Interrupt Controller Support 85



3.10 Serial Interrupt (D31:F0) 85
3.10.1 Start Frame 86
3.10.2 Data Frames 86
3.10.3 Stop Frame 87
3.10.4 Specific Interrupts Not Supported Using SERIRQ 87
3.10.5 Data Frame Format 87
3.11 Real Time Clock (D31:F0) 88
3.11.1 Update Cycles 89
3.11.2 Interrupts 89
3.11.3 Lockable RAM Ranges 89
3.11.4 Century Rollover 89
3.11.5 Clearing Battery-Backed RTC RAM 90
3.12 Power Management 91
3.12.1 Features 91
3.12.2 Intel® Xeon® Processor D-1500 Product Family and System Power States 92
3.12.3 System Power Planes 93
3.12.4 SMI# / SCI Generation 94
3.12.5 C-States 97
3.12.6 Sleep States 97
3.12.7 Event Input Signals and Their Usage 100
3.12.8 ALT Access Mode 103
3.12.9 System Power Supplies, Planes, and Signals 106
3.12.10 Legacy Power Management Theory of Operation 110
3.12.11 Reset Behavior 110
3.13 System Management (D31:F0) 112
3.13.1 Theory of Operation 112
3.13.2 TCO Modes 114
3.14 General Purpose I/O (D31:F0) 115
3.14.1 Power Wells 115
3.14.2 SMI# SCI and NMI Routing 115
3.14.3 Triggering 115
3.14.4 GPIO Registers Lockdown 116
3.14.5 Serial POST Codes over GPIO 116
3.15 SATA Host Controller (D31:F2, F5) 119
3.15.1 SATA 6 Gb/s Support 119
3.15.2 SATA Feature Support 120
3.15.3 Theory of Operation 120
3.15.4 SATA Swap Bay Support 121
3.15.5 Hot-Plug Operation 121
3.15.6 Function Level Reset Support (FLR) 121
3.15.7 Power Management Operation 122
3.15.8 SATA Device Presence 124
3.15.9 SATA LED 124
3.15.10 AHCI Operation 125
3.15.11 SGPIO Signals 125
3.16 High Precision Event Timers (HPET) 129
3.16.1 Timer Accuracy 129
3.16.2 Interrupt Mapping 129
3.16.3 Periodic versus Non-Periodic Modes 130
3.16.4 Enabling the Timers 131
3.16.5 Interrupt Levels 131
3.16.6 Handling Interrupts 132
3.16.7 Issues Related to 64-Bit Timers with 32-Bit Processors 132
3.17 USB EHCI Host Controllers (D29:F0) 132
3.17.1 EHC Initialization 133
3.17.2 Data Structures in Main Memory 133
3.17.3 USB 2.0 Enhanced Host Controller DMA 133
3.17.4 Data Encoding and Bit Stuffing 134
3.17.5 Packet Formats 134
3.17.6 USB 2.0 Interrupts and Error Conditions 134
3.17.7 USB 2.0 Power Management 135
3.17.8 USB 2.0 Legacy Keyboard Operation 136
3.17.9 USB 2.0 Based Debug Port 136
3.17.10 EHCI Caching 141
3.17.11 Intel® USB Pre-Fetch Based Pause 141

3.17.12 Function Level Reset Support (FLR) 142
3.17.13 USB Overcurrent Protection 142
3.18 Integrated USB 2.0 Rate Matching Hub 143
3.18.1 Overview 143
3.18.2 Architecture 143
3.19 xHCI Controller (D20:F0) 144
3.20 SMBus Controller (D31:F3) 144
3.20.1 Host Controller 145
3.20.2 Bus Arbitration 149
3.20.3 Bus Timing 150
3.20.4 Interrupts / SMI# 150
3.20.5 SMBALERT# 151
3.20.6 SMBus CRC Generation and Checking 151
3.20.7 SMBus Slave Interface 151
3.21 Thermal Management 157
3.21.1 Thermal Sensor 157
3.21.2 Intel® Xeon® Processor D-1500 Product Family Thermal Throttling 159
3.21.3 Thermal Reporting Over System Management Link 1 Interface (SMLink0) 159
3.22 Intel® Management Engine (Intel® ME) and Intel® Management Engine Firmware (Intel® ME FW) 9.0 165
3.22.1 Intel® ME Requirements 166
3.23 Serial Peripheral Interface (SPI) 167
3.23.1 SPI Supported Feature Overview 168
3.23.2 Flash Descriptor 169
3.23.3 Flash Access 171
3.23.4 Serial Flash Device Compatibility Requirements 172
3.23.5 Multiple Page Write Usage Model 175
3.23.6 Flash Device Configurations 176
3.23.7 SPI Flash Device Recommended Pinout 176
3.23.8 Serial Flash Device Package 177
3.23.9 PWM Outputs 178
3.23.10 TACH Inputs 178
3.24 Feature Capability Mechanism 178
3.25 Intel® Virtualization Technology (Intel® VT) 179
3.25.1 Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d) Objectives 179
3.25.2 Intel® VT-d Features Supported 179
3.25.3 Support for Function Level Reset (FLR) in Intel® Xeon® Processor D-1500 Product Family 179
3.25.4 Virtualization Support for Intel® Xeon® Processor D-1500 Product Family IOxAPIC 180
3.25.5 Virtualization Support for High Precision Event Timer (HPET) 180

4 Register and Memory Mapping 181
4.1 PCI Devices and Functions 182
4.2 PCI Configuration Map 183
4.3 I/O Map 183
4.3.1 Fixed I/O Address Ranges 183
4.3.2 Variable I/O Decode Ranges 185
4.4 Memory Map 186
4.4.1 Boot-Block Update Scheme 188

5 Chipset Configuration Registers 190
5.1 Chipset Configuration Registers (Memory Space) 190
5.1.1 RPC—Root Port Configuration Register 191
5.1.2 RPFN—Root Port Function Number and Hide for PCI Express* Root Ports Register 191
5.1.3 FLRSTAT—Function Level Reset Pending Status Register 193
5.1.4 TRSR—Trap Status Register 193
5.1.5 TRCR—Trapped Cycle Register 193
5.1.6 TWDR—Trapped Write Data Register 194
5.1.7 IOTRn—I/O Trap Register (0–3) 194
5.1.8 V0CTL—Virtual Channel 0 Resource Control Register 195
5.1.9 V0STS—Virtual Channel 0 Resource Status Register 195
5.1.10 V1CTL—Virtual Channel 1 Resource Control Register 195
5.1.11 V1STS—Virtual Channel 1 Resource Status Register 196

5.1.12 REC—Root Error Command Register 196
5.1.13 CIR2314—Chipset Initialization Register 2314 196
5.1.14 CIR2320—Chipset Initialization Register 2320 196
5.1.15 TCTL—TCO Configuration Register 196
5.1.16 D31IP—Device 31 Interrupt Pin Register 197
5.1.17 D30IP—Device 30 Interrupt Pin Register 198
5.1.18 D29IP—Device 29 Interrupt Pin Register 198
5.1.19 D28IP—Device 28 Interrupt Pin Register 198
5.1.20 D27IP—Device 27 Interrupt Pin Register 199
5.1.21 D26IP—Device 26 Interrupt Pin Register 199
5.1.22 D25IP—Device 25 Interrupt Pin Register 200
5.1.23 D22IP—Device 22 Interrupt Pin Register 200
5.1.24 D20IP—Device 20 Interrupt Pin Register 201
5.1.25 D31IR—Device 31 Interrupt Route Register 201
5.1.26 D30IR—Device 30 Interrupt Route Register 202
5.1.27 D29IR—Device 29 Interrupt Route Register 202
5.1.28 D28IR—Device 28 Interrupt Route Register 203
5.1.29 D27IR—Device 27 Interrupt Route Register 204
5.1.30 D26IR—Device 26 Interrupt Route Register 205
5.1.31 D25IR—Device 25 Interrupt Route Register 206
5.1.32 D22IR—Device 22 Interrupt Route Register 207
5.1.33 D20IR—Device 20 Interrupt Route Register 208
5.1.34 OIC—Other Interrupt Control Register 209
5.1.35 WADT_AC—Wake Alarm Device Timer – AC Register 209
5.1.36 WADT_DC—Wake Alarm Device Timer – DC Register 209
5.1.37 WADT_EXP_AC—Wake Alarm Device Expired Timer – AC Register 210
5.1.38 WADT_EXP_DC—Wake Alarm Device Expired Timer: DC Register 210
5.1.39 PRSTS—Power and Reset Status Register 210
5.1.40 CIR3314—Chipset Initialization Register 3314 211
5.1.41 PM_CFG—Power Management Configuration Register 211
5.1.42 CIR3324—Chipset Initialization Register 3324 213
5.1.43 DCIR3340—Chipset Initialization Register 3340 213
5.1.44 CIR3344—Chipset Initialization Register 3344 213
5.1.45 CIR3348—Chipset Initialization Register 3348 213
5.1.46 CIR3350—Chipset Initialization Register 3350 213
5.1.47 CIR3360—Chipset Initialization Register 3360 214
5.1.48 CIR3368—Chipset Initialization Register 3368 214
5.1.49 CIR3378—Chipset Initialization Register 3378 214
5.1.50 CIR337C—Chipset Initialization Register 337C 214
5.1.51 CIR3388—Chipset Initialization Register 3388 214
5.1.52 CIR3390—Chipset Initialization Register 3390 215
5.1.53 CIR33A0—Chipset Initialization Register 33A0 215
5.1.54 CIR33B0—Chipset Initialization Register 33B0 215
5.1.55 CIR33C0—Chipset Initialization Register 33C0 215
5.1.56 PMSYNC_CFG—PMSYNC Configuration 215
5.1.57 CIR33D0—Chipset Initialization Register 33D0 216
5.1.58 CIR33D4—Chipset Initialization Register 33D4 216
5.1.59 RC—RTC Configuration Register 216
5.1.60 HPTC—High Precision Timer Configuration Register 217
5.1.61 GCS—General Control and Status Register 217
5.1.62 BUC—Backed Up Control Register 218
5.1.63 FD—Function Disable Register 219
5.1.64 CG—Clock Gating Register 220
5.1.65 DISPBDF—Display Bus, Device and Function Initialization Register 221
5.1.66 FD2—Function Disable 2 Register 221
5.1.67 CIR3A28—Chipset Initialization Register 3A28 222
5.1.68 CIR3A2C—Chipset Initialization Register 3A2C 222
5.1.69 CIR3A6C—Chipset Initialization Register 3A6C 222
5.1.70 CIR3A80—Chipset Initialization Register 3A80 222
5.1.71 CIR3A84—Chipset Initialization Register 3A84 222
5.1.72 CIR3A88—Chipset Initialization Register 3A88 222
5.2 Thermal Configuration Registers 223
5.2.1 TIRC0—Thermal Initialization Register C0 223
5.2.2 TIRC4—Thermal Initialization Register C4 223
5.2.3 TIRC8—Thermal Initialization Register C8 223
5.2.4 TIRCC—Thermal Initialization Register CC 223
5.2.5 TIRD0—Thermal Initialization Register D0 224

5.2.6 TIRE0—Thermal Initialization Register E0 224
5.2.7 TIRF0—Thermal Initialization Register F0 224

6 Gigabit LAN Configuration Registers 225
6.1 Gigabit LAN Configuration Registers (Gigabit LAN—D25:F0) 225
6.1.1 VID—Vendor Identification Register (Gigabit LAN—D25:F0) 226
6.1.2 DID—Device Identification Register (Gigabit LAN—D25:F0) 226
6.1.3 PCICMD—PCI Command Register (Gigabit LAN—D25:F0) 226
6.1.4 PCISTS—PCI Status Register (Gigabit LAN—D25:F0) 227
6.1.5 RID—Revision Identification Register (Gigabit LAN—D25:F0) 228
6.1.6 CC—Class Code Register (Gigabit LAN—D25:F0) 228
6.1.7 CLS—Cache Line Size Register (Gigabit LAN—D25:F0) 228
6.1.8 PLT—Primary Latency Timer Register (Gigabit LAN—D25:F0) 228
6.1.9 HEADTYP—Header Type Register (Gigabit LAN—D25:F0) 228
6.1.10 MBARA—Memory Base Address Register A (Gigabit LAN—D25:F0) 229
6.1.11 MBARB—Memory Base Address Register B (Gigabit LAN—D25:F0) 229
6.1.12 MBARC—Memory Base Address Register C (Gigabit LAN—D25:F0) 229
6.1.13 SVID—Subsystem Vendor ID Register (Gigabit LAN—D25:F0) 230
6.1.14 SID—Subsystem ID Register (Gigabit LAN—D25:F0) 230
6.1.15 ERBA—Expansion ROM Base Address Register (Gigabit LAN—D25:F0) 230
6.1.16 CAPP—Capabilities List Pointer Register (Gigabit LAN—D25:F0) 230
6.1.17 INTR—Interrupt Information Register (Gigabit LAN—D25:F0) 230
6.1.18 MLMG—Maximum Latency / Minimum Grant Register (Gigabit LAN—D25:F0) 231
6.1.19 STCL—System Time Control Low Register (Gigabit LAN—D25:F0) 231
6.1.20 STCH—System Time Control High Register (Gigabit LAN—D25:F0) 231
6.1.21 LTRCAP—System Time Control High Register (Gigabit LAN—D25:F0) 231
6.1.22 CLIST1—Capabilities List Register 1 (Gigabit LAN—D25:F0) 232
6.1.23 PMC—PCI Power Management Capabilities Register (Gigabit LAN—D25:F0) 232
6.1.24 PMCS—PCI Power Management Control and Status Register (Gigabit LAN—D25:F0) 233
6.1.25 DR—Data Register (Gigabit LAN—D25:F0) 233
6.1.26 CLIST2—Capabilities List Register 2 (Gigabit LAN—D25:F0) 234
6.1.27 MCTL—Message Control Register (Gigabit LAN—D25:F0) 234
6.1.28 MADDL—Message Address Low Register (Gigabit LAN—D25:F0) 234
6.1.29 MADDH—Message Address High Register (Gigabit LAN—D25:F0) 234
6.1.30 MDAT—Message Data Register (Gigabit LAN—D25:F0) 235
6.1.31 FLRCAP—Function Level Reset Capability (Gigabit LAN—D25:F0) 235
6.1.32 FLRCLV—Function Level Reset Capability Length and Version Register (Gigabit LAN—D25:F0) 235
6.1.33 DEVCTRL—Device Control Register (Gigabit LAN—D25:F0) 236
6.2 Gigabit LAN Capabilities and Status Registers (CSR) 236
6.2.1 GBECSR_00—Gigabit Ethernet Capabilities and Status Register 00 237
6.2.2 GBECSR_18—Gigabit Ethernet Capabilities and Status Register 18 237
6.2.3 GBECSR_20—Gigabit Ethernet Capabilities and Status Register 20 237
6.2.4 GBECSR_2C—Gigabit Ethernet Capabilities and Status Register 2C 238
6.2.5 GBECSR_F00—Gigabit Ethernet Capabilities and Status Register F00 238
6.2.6 GBECSR_F10—Gigabit Ethernet Capabilities and Status Register F10 238
6.2.7 GBECSR_5400—Gigabit Ethernet Capabilities and Status Register 5400 239
6.2.8 GBECSR_5404—Gigabit Ethernet Capabilities and Status Register 5404 239
6.2.9 GBECSR_5800—Gigabit Ethernet Capabilities and Status Register 5800 239
6.2.10 GBECSR_5B54—Gigabit Ethernet Capabilities and Status Register 5B54 239

7 LPC Interface Bridge Registers (D31:F0) 240
7.1 PCI Configuration Registers (LPC I/F—D31:F0) 240
7.1.1 VID—Vendor Identification Register (LPC I/F—D31:F0) 241
7.1.2 DID—Device Identification Register (LPC I/F—D31:F0) 241
7.1.3 PCICMD—PCI COMMAND Register (LPC I/F—D31:F0) 241
7.1.4 PCISTS—PCI Status Register (LPC I/F—D31:F0) 242
7.1.5 RID—Revision Identification Register (LPC I/F—D31:F0) 243
7.1.6 PI—Programming Interface Register (LPC I/F—D31:F0) 243
7.1.7 SCC—Sub Class Code Register (LPC I/F—D31:F0) 243
7.1.8 BCC—Base Class Code Register (LPC I/F—D31:F0) 243
7.1.9 PLT—Primary Latency Timer Register (LPC I/F—D31:F0) 243
7.1.10 HEADTYP—Header Type Register (LPC I/F—D31:F0) 243
7.1.11 SS—Sub System Identifiers Register (LPC I/F—D31:F0) 244
7.1.12 CAPP—Capability List Pointer Register (LPC I/F—D31:F0) 244
7.1.13 PMBASE—ACPI Base Address Register (LPC I/F—D31:F0) 244

7.1.14 ACPI_CNTL—ACPI Control Register (LPC I/F — D31:F0) 244
7.1.15 GPIOBASE—GPIO Base Address Register (LPC I/F — D31:F0) 245
7.1.16 GC—GPIO Control Register (LPC I/F — D31:F0) 245
7.1.17 PIRQ[n]_ROUT—PIRQ[A,B,C,D] Routing Control Register (LPC I/F—D31:F0) 246
7.1.18 SIRQ_CNTL—Serial IRQ Control Register (LPC I/F—D31:F0) 247
7.1.19 PIRQ[n]_ROUT—PIRQ[E,F,G,H] Routing Control Register (LPC I/F—D31:F0) 247
7.1.20 LPC_IBDF—IOxAPIC Bus:Device:Function (LPC I/F—D31:F0) 248
7.1.21 LPC_HnBDF—HPET n Bus:Device:Function (LPC I/F—D31:F0) 248
7.1.22 LPC_I/O_DEC—I/O Decode Ranges Register (LPC I/F—D31:F0)..... 249
7.1.23 LPC_EN—LPC I/F Enables Register (LPC I/F—D31:F0) 249
7.1.24 GEN1_DEC—LPC I/F Generic Decode Range 1 Register (LPC I/F—D31:F0) 250
7.1.25 GEN2_DEC—LPC I/F Generic Decode Range 2 Register (LPC I/F—D31:F0) 251
7.1.26 GEN3_DEC—LPC I/F Generic Decode Range 3 Register (LPC I/F—D31:F0) 251
7.1.27 GEN4_DEC—LPC I/F Generic Decode Range 4 Register (LPC I/F—D31:F0) 251
7.1.28 ULKMC—USB Legacy Keyboard / Mouse Control Register (LPC I/F—D31:F0) 252
7.1.29 LGMR—LPC I/F Generic Memory Range Register (LPC I/F—D31:F0) 253
7.1.30 BIOS_SEL1—BIOS Select 1 Register (LPC I/F—D31:F0) 253
7.1.31 BIOS_SEL2—BIOS Select 2 Register (LPC I/F—D31:F0) 254
7.1.32 BIOS_DEC_EN1—BIOS Decode Enable Register (LPC I/F—D31:F0) 254
7.1.33 BIOS_CNTL—BIOS Control Register (LPC I/F—D31:F0) 256
7.1.34 FDCAP—Feature Detection Capability ID Register (LPC I/F—D31:F0)..... 257
7.1.35 FDLEN—Feature Detection Capability Length Register (LPC I/F—D31:F0)..... 257
7.1.36 FDVER—Feature Detection Version Register (LPC I/F—D31:F0) 257
7.1.37 FVECIDX—Feature Vector Index Register (LPC I/F—D31:F0)..... 257
7.1.38 FVECD—Feature Vector Data Register (LPC I/F—D31:F0) 258
7.1.39 Feature Vector Space 258
7.1.40 RCBA—Root Complex Base Address Register (LPC I/F—D31:F0) 259
7.2 DMA I/O Registers 259
7.2.1 DMABASE_CA—DMA Base and Current Address Registers..... 261
7.2.2 DMABASE_CC—DMA Base and Current Count Registers..... 261
7.2.3 DMAMEM_LP—DMA Memory Low Page Registers 262
7.2.4 DMACMD—DMA Command Register..... 262
7.2.5 DMASTA—DMA Status Register..... 262
7.2.6 DMA_WRSMSK—DMA Write Single Mask Register 263
7.2.7 DMACH_MODE—DMA Channel Mode Register..... 263
7.2.8 DMA Clear Byte Pointer Register 264
7.2.9 DMA Master Clear Register..... 264
7.2.10 DMA_CLMSK—DMA Clear Mask Register..... 264
7.2.11 DMA_WRMSK—DMA Write All Mask Register 264
7.3 Timer I/O Registers 265
7.3.1 TCW—Timer Control Word Register 265
7.3.2 SBYTE_FMT—Interval Timer Status Byte Format Register 267
7.3.3 Counter Access Ports Register 268
7.4 8259 Interrupt Controller (PIC) Registers..... 268
7.4.1 Interrupt Controller I/O MAP 268
7.4.2 ICW1—Initialization Command Word 1 Register 269
7.4.3 ICW2—Initialization Command Word 2 Register 270
7.4.4 ICW3—Master Controller Initialization Command Word 3 Register..... 270
7.4.5 ICW3—Slave Controller Initialization Command Word 3 Register 271
7.4.6 ICW4—Initialization Command Word 4 Register 271
7.4.7 OCW1—Operational Control Word 1 (Interrupt Mask) Register 271
7.4.8 OCW2—Operational Control Word 2 Register 272
7.4.9 OCW3—Operational Control Word 3 Register 272
7.4.10 ELCR1—Master Controller Edge/Level Triggered Register..... 273
7.4.11 ELCR2—Slave Controller Edge/Level Triggered Register..... 274
7.5 Advanced Programmable Interrupt Controller (APIC) 274
7.5.1 APIC Register Map 274
7.5.2 IND—Index Register..... 275
7.5.3 DAT—Data Register..... 275
7.5.4 EOIR—EOI Register..... 275
7.5.5 ID—Identification Register 276
7.5.6 VER—Version Register..... 276
7.5.7 REDIR_TBL—Redirection Table Register 277
7.6 Real Time Clock Registers..... 278
7.6.1 I/O Register Address Map 278
7.6.2 Indexed Registers..... 279
7.7 Processor Interface Registers 282

7.7.1 NMI_SC—NMI Status and Control Register 282
7.7.2 NMI_EN—NMI Enable (and Real Time Clock Index) Register 283
7.7.3 PORT92—Init Register 283
7.7.4 COPROC_ERR—Coprocessor Error Register 283
7.7.5 RST_CNT—Reset Control Register 284
7.8 Power Management Registers 284
7.8.1 Power Management PCI Configuration Registers (PM—D31:F0) 284
7.8.2 APM I/O Decode Register 292
7.8.3 Power Management I/O Registers 293
7.9 System Management TCO Registers 307
7.9.1 TCO_RLD—TCO Timer Reload and Current Value Register 308
7.9.2 TCO_DAT_IN—TCO Data In Register 308
7.9.3 TCO_DAT_OUT—TCO Data Out Register 308
7.9.4 TCO1_STS—TCO1 Status Register 309
7.9.5 TCO2_STS—TCO2 Status Register 310
7.9.6 TCO1_CNT—TCO1 Control Register 311
7.9.7 TCO2_CNT—TCO2 Control Register 311
7.9.8 TCO_MESSAGE1 and TCO_MESSAGE2 Registers 312
7.9.9 TCO_WDCNT—TCO Watchdog Control Register 312
7.9.10 SW_IRQ_GEN—Software IRQ Generation Register 312
7.9.11 TCO_TMR—TCO Timer Initial Value Register 313
7.10 General Purpose I/O Registers 313
7.10.1 GPIO_USE_SEL—GPIO Use Select Register 314
7.10.2 GP_IO_SEL—GPIO Input/Output Select Register 315
7.10.3 GP_LVL—GPIO Level for Input or Output Register 315
7.10.4 GPO_BLINK—GPO Blink Enable Register 316
7.10.5 GP_SER_BLINK—GP Serial Blink Register 316
7.10.6 GP_SB_CMDSTS—GP Serial Blink Command Status Register 317
7.10.7 GP_SB_DATA—GP Serial Blink Data Register 317
7.10.8 GPI_NMI_EN—GPI NMI Enable Register 318
7.10.9 GPI_NMI_STS—GPI NMI Status Register 318
7.10.10 GPI_INV—GPIO Signal Invert Register 319
7.10.11 GPIO_USE_SEL2—GPIO Use Select 2 Register 319
7.10.12 GP_IO_SEL2—GPIO Input/Output Select 2 Register 320
7.10.13 GP_LVL2—GPIO Level for Input or Output 2 Register 320
7.10.14 GPI_NMI_EN_2—GPI NMI Enable Register 2 320
7.10.15 GPI_NMI_STS_2—GPI NMI Status Register 2 321
7.10.16 GPIO_USE_SEL3—GPIO Use Select 3 Register 321
7.10.17 GP_IO_SEL3—GPIO Input/Output Select 3 Register 322
7.10.18 GP_LVL3—GPIO Level for Input or Output 3 Register 322
7.10.19 GPI_NMI_EN_3—GPI NMI Enable Register 3 323
7.10.20 GPI_NMI_STS_3—GPI NMI Status Register 3 323
7.10.21 GP_RST_SEL1 — GPIO Reset Select Register 323
7.10.22 GP_RST_SEL2—GPIO Reset Select Register 324
7.10.23 GP_RST_SEL3—GPIO Reset Select Register 324

8 SATA Controller Registers (D31:F2) 325
8.1 PCI Configuration Registers (SATA–D31:F2) 325
8.1.1 VID—Vendor Identification Register (SATA—D31:F2) 326
8.1.2 DID—Device Identification Register (SATA—D31:F2) 326
8.1.3 PCICMD—PCI Command Register (SATA–D31:F2) 327
8.1.4 PCISTS — PCI Status Register (SATA–D31:F2) 327
8.1.5 RID—Revision Identification Register (SATA—D31:F2) 328
8.1.6 PI—Programming Interface Register (SATA–D31:F2) 328
8.1.7 SCC—Sub Class Code Register (SATA–D31:F2) 329
8.1.8 BCC—Base Class Code Register (SATA–D31:F2SATA–D31:F2) 329
8.1.9 PMLT—Primary Master Latency Timer Register (SATA–D31:F2) 329
8.1.10 HTYPE—Header Type Register (SATA–D31:F2) 329
8.1.11 PCMD_BAR—Primary Command Block Base Address Register (SATA–D31:F2) 330
8.1.12 PCNL_BAR—Primary Control Block Base Address Register (SATA–D31:F2) 330
8.1.13 SCMD_BAR—Secondary Command Block Base Address Register (SATA D31:F2) 330
8.1.14 SCNL_BAR—Secondary Control Block Base Address Register (SATA D31:F2) 331
8.1.15 BAR—Legacy Bus Master Base Address Register (SATA–D31:F2) 331
8.1.16 ABAR/SIDPBA1—AHCI Base Address Register / Serial ATA Index Data Pair Base Address (SATA–D31:F2) 331

8.1.17 SVID—Subsystem Vendor Identification Register (SATA–D31:F2) 332
8.1.18 SID—Subsystem Identification Register (SATA–D31:F2)..... 332
8.1.19 CAP—Capabilities Pointer Register (SATA–D31:F2) 333
8.1.20 INT_LN—Interrupt Line Register (SATA–D31:F2)..... 333
8.1.21 INT_PN—Interrupt Pin Register (SATA–D31:F2) 333
8.1.22 IDE_TIM—IDE Timing Register (SATA–D31:F2)..... 333
8.1.23 SIDETIM—Slave IDE Timing Register (SATA–D31:F2) 334
8.1.24 SDMA_CNT—Synchronous DMA Control Register (SATA–D31:F2) 334
8.1.25 SDMA_TIM—Synchronous DMA Timing Register (SATA–D31:F2)..... 334
8.1.26 IDE_CONFIG—IDE I/O Configuration Register (SATA–D31:F2) 335
8.1.27 PID—PCI Power Management Capability Identification Register (SATA–D31:F2) 335
8.1.28 PC—PCI Power Management Capabilities Register (SATA–D31:F2)..... 335
8.1.29 PMCS—PCI Power Management Control and Status Register (SATA–D31:F2)..... 336
8.1.30 MSICI—Message Signaled Interrupt Capability Identification Register (SATA–D31:F2) 336
8.1.31 MSIMC—Message Signaled Interrupt Message Control Register (SATA–D31:F2) 337
8.1.32 MSIMA— Message Signaled Interrupt Message Address Register (SATA–D31:F2) 338
8.1.33 MSIMD—Message Signaled Interrupt Message Data Register (SATA–D31:F2)..... 338
8.1.34 MAP—Address Map Register (SATA–D31:F2)..... 338
8.1.35 PCS—Port Control and Status Register (SATA–D31:F2) 339
8.1.36 SCLKCG—SATA Clock Gating Control Register..... 341
8.1.37 SGC—SATA General Configuration Register 341
8.1.38 SATACR0—SATA Capability Register 0 (SATA–D31:F2)..... 342
8.1.39 SATACR1—SATA Capability Register 1 (SATA–D31:F2)..... 342
8.1.40 FLRCID—FLR Capability Identification Register (SATA–D31:F2) 343
8.1.41 FLRCLV—FLR Capability Length and Version Register (SATA–D31:F2) 343
8.1.42 FLRC—FLR Control Register (SATA–D31:F2) 343
8.1.43 ATC—APM Trapping Control Register (SATA–D31:F2)..... 344
8.1.44 ATS—APM Trapping Status Register (SATA–D31:F2)..... 344
8.1.45 SP—Scratch Pad Register (SATA–D31:F2) 344
8.1.46 BFCS—BIST FIS Control/Status Register (SATA–D31:F2)..... 345
8.1.47 BFTD1—BIST FIS Transmit Data1 Register (SATA–D31:F2) 346
8.1.48 BFTD2—BIST FIS Transmit Data2 Register (SATA–D31:F2) 346
8.2 Bus Master IDE I/O Registers (D31:F2) 347
8.2.1 BMIC[P,S]—Bus Master IDE Command Register (D31:F2)..... 347
8.2.2 BMIS[P,S]—Bus Master IDE Status Register (D31:F2)..... 348
8.2.3 BMID[P,S]—Bus Master IDE Descriptor Table Pointer Register (D31:F2) 349
8.2.4 AIR—AHCI Index Register (D31:F2) 349
8.2.5 AIDR—AHCI Index Data Register (D31:F2)..... 349
8.3 Serial ATA Index/Data Pair Superset Registers 349
8.3.1 SINDX—Serial ATA Index Register (D31:F2) 350
8.3.2 SDATA—Serial ATA Data Register (D31:F2) 350
8.4 AHCI Registers (D31:F2) 353
8.4.1 AHCI Generic Host Control Registers (D31:F2)..... 354
8.4.2 Port Registers (D31:F2)..... 359

9 SATA Controller Registers (D31:F5)..... 373
9.1 PCI Configuration Registers (SATA–D31:F5)..... 373
9.1.1 VID—Vendor Identification Register (SATA—D31:F5) 374
9.1.2 DID—Device Identification Register (SATA—D31:F5) 374
9.1.3 PCICMD—PCI Command Register (SATA–D31:F5) 374
9.1.4 PCISTS — PCI Status Register (SATA–D31:F5) 375
9.1.5 RID—Revision Identification Register (SATA—D31:F5) 376
9.1.6 PI—Programming Interface Register (SATA–D31:F5) 376
9.1.7 SCC—Sub Class Code Register (SATA–D31:F5)..... 376
9.1.8 BCC—Base Class Code Register (SATA–D31:F5SATA–D31:F5) 376
9.1.9 PCMD_BAR—Primary Command Block Base Address Register (SATA–D31:F5) 377
9.1.10 PCNL_BAR—Primary Control Block Base Address Register (SATA–D31:F5)..... 377
9.1.11 SCMD_BAR—Secondary Command Block Base Address Register (SATA D31:F5) 377
9.1.12 SCNL_BAR—Secondary Control Block Base Address Register (SATA D31:F5)..... 378
9.1.13 BAR — Legacy Bus Master Base Address Register (SATA–D31:F5) 378
9.1.14 SIDPBA — SATA Index/Data Pair Base Address Register (SATA–D31:F5)..... 378
9.1.15 SVID—Subsystem Vendor Identification Register (SATA–D31:F5)..... 379

9.1.16 SID—Subsystem Identification Register (SATA–D31:F5) 379
9.1.17 CAP—Capabilities Pointer Register (SATA–D31:F5) 379
9.1.18 INT_LN—Interrupt Line Register (SATA–D31:F5) 379
9.1.19 INT_PN—Interrupt Pin Register (SATA–D31:F5) 379
9.1.20 IDE_TIM—IDE Timing Register (SATA–D31:F5) 380
9.1.21 SDMA_CNT—Synchronous DMA Control Register (SATA–D31:F5) 380
9.1.22 SDMA_TIM—Synchronous DMA Timing Register (SATA–D31:F5) 380
9.1.23 IDE_CONFIG—IDE I/O Configuration Register (SATA–D31:F5) 381
9.1.24 PID—PCI Power Management Capability Identification Register (SATA–D31:F5) 381
9.1.25 PC—PCI Power Management Capabilities Register (SATA–D31:F5) 381
9.1.26 PMCS—PCI Power Management Control and Status Register (SATA–D31:F5) 382
9.1.27 MAP—Address Map Register (SATA–D31:F5) 383
9.1.28 PCS—Port Control and Status Register (SATA–D31:F5) 383
9.1.29 SATACR0—SATA Capability Register 0 (SATA–D31:F5) 384
9.1.30 SATACR1—SATA Capability Register 1 (SATA–D31:F5) 384
9.1.31 FLRCID—FLR Capability ID Register (SATA–D31:F5) 384
9.1.32 FLRCLV—FLR Capability Length and Value Register (SATA–D31:F5) 385
9.1.33 FLRCTRL—FLR Control Register (SATA–D31:F5) 385
9.1.34 ATC—APM Trapping Control Register (SATA–D31:F5) 385
9.1.35 ATC—APM Trapping Control Register (SATA–D31:F5) 385
9.2 Bus Master IDE I/O Registers (D31:F5) 386
9.2.1 BMIC[P,S]—Bus Master IDE Command Register (D31:F5) 386
9.2.2 BMIS[P,S]—Bus Master IDE Status Register (D31:F5) 387
9.2.3 BMID[P,S]—Bus Master IDE Descriptor Table Pointer Register (D31:F5) 388
9.3 Serial ATA Index/Data Pair Superset Registers 388
9.3.1 SINDX—SATA Index Register (D31:F5) 388
9.3.2 SDATA—SATA Index Data Register (D31:F5) 389

10 EHCI Controller Registers (D29:F0) 393
10.1 USB EHCI Configuration Registers (USB EHCI—D29:F0) 393
10.1.1 VID—Vendor Identification Register (USB EHCI—D29:F0) 394
10.1.2 DID—Device Identification Register (USB EHCI—D29:F0) 394
10.1.3 PCICMD—PCI Command Register (USB EHCI—D29:F0) 394
10.1.4 PCISTS—PCI Status Register (USB EHCI—D29:F0) 395
10.1.5 RID—Revision Identification Register (USB EHCI—D29:F0) 396
10.1.6 PI—Programming Interface Register (USB EHCI—D29:F0) 396
10.1.7 SCC—Sub Class Code Register (USB EHCI—D29:F0) 396
10.1.8 BCC—Base Class Code Register (USB EHCI—D29:F0) 397
10.1.9 PMLT—Primary Master Latency Timer Register (USB EHCI—D29:F0) 397
10.1.10 HEADTYP—Header Type Register (USB EHCI—D29:F0) 397
10.1.11 MEM_BASE—Memory Base Address Register (USB EHCI—D29:F0) 397
10.1.12 SVID—USB EHCI Subsystem Vendor ID Register (USB EHCI—D29:F0) 398
10.1.13 SID—USB EHCI Subsystem ID Register (USB EHCI—D29:F0) 398
10.1.14 CAP_PTR—Capabilities Pointer Register (USB EHCI—D29:F0) 398
10.1.15 INT_LN—Interrupt Line Register (USB EHCI—D29:F0) 398
10.1.16 INT_PN—Interrupt Pin Register (USB EHCI—D29:F0) 399
10.1.17 PWR_CAPID—PCI Power Management Capability Identification Register (USB EHCI—D29:F0) 399
10.1.18 NXT_PTR1—Next Item Pointer #1 Register (USB EHCI—D29:F0) 399
10.1.19 PWR_CAP—Power Management Capabilities Register (USB EHCI—D29:F0) 399
10.1.20 PWR_CNTL_STS—Power Management Control / Status Register (USB EHCI—D29:F0) 400
10.1.21 DEBUG_CAPID—Debug Port Capability ID Register (USB EHCI—D29:F0) 401
10.1.22 NXT_PTR2—Next Item Pointer #2 Register (USB EHCI—D29:F0) 401
10.1.23 DEBUG_BASE—Debug Port Base Offset Register (USB EHCI—D29:F0) 401
10.1.24 USB_RELNUM—USB Release Number Register (USB EHCI—D29:F0) 401
10.1.25 FL_ADJ—Frame Length Adjustment Register (USB EHCI—D29:F0) 401
10.1.26 PWAKE_CAP—Port Wake Capability Register (USB EHCI—D29:F0) 402
10.1.27 PDO—Port Disable Override Register 403
10.1.28 RMHDEVR—RMH Device Removable Field Register 403
10.1.29 LEG_EXT_CAP—USB EHCI Legacy Support Extended Capability Register (USB EHCI—D29:F0) 403
10.1.30 LEG_EXT_CS—USB EHCI Legacy Support Extended Control / Status Register (USB EHCI—D29:F0) 404
10.1.31 SPECIAL_SMI—Intel® Specific USB 2.0 SMI Register (USB EHCI—D29:F0) 405
10.1.32 OCMAP—Over-Current Mapping Register 406

10.1.33 RMHWKCTL—RMH Wake Control Register 407
10.1.34 ACCESS_CNTL—Access Control Register (USB EHCI—D29:F0) 408
10.1.35 EHCIIR1—EHCI Initialization Register 1 (USB EHCI—D29:F0) 408
10.1.36 FLR_CID—Function Level Reset Capability ID Register (USB EHCI—D29:F0) 408
10.1.37 FLR_NEXT—Function Level Reset Next Capability Pointer Register (USB EHCI—D29:F0) 409
10.1.38 FLR_CLV—Function Level Reset Capability Length and Version Register (USB EHCI—D29:F0) 409
10.1.39 FLR_CTRL—Function Level Reset Control Register (USB EHCI—D29:F0) 409
10.1.40 FLR_STS—Function Level Reset Status Register (USB EHCI—D29:F0) 409
10.2 Memory-Mapped I/O Registers 410
10.2.1 Host Controller Capability Registers 410
10.2.2 Host Controller Operational Registers 412
10.2.3 USB 2.0-Based Debug Port Registers 423

11 xHCI Controller Registers (D20:F0) 426
11.1 USB xHCI Configuration Registers (USB xHCI—D20:F0) 426
11.2 VID—Vendor Identification Register (USB xHCI—D20:F0) 427
11.2.1 DID—Device Identification Register (USB xHCI—D20:F0) 427
11.2.2 PCICMD—PCI Command Register (USB xHCI—D20:F0) 427
11.2.3 PCISTS—PCI Status Register (USB xHCI—D20:F0) 428
11.2.4 RID—Revision Identification Register (USB xHCI—D20:F0) 429
11.2.5 PI—Programming Interface Register (USB xHCI—D20:F0) 429
11.2.6 SCC—Sub Class Code Register (USB xHCI—D20:F0) 429
11.2.7 BCC—Base Class Code Register (USB xHCI—D20:F0) 429
11.2.8 PMLT—Primary Master Latency Timer Register (USB xHCI—D20:F0) 430
11.2.9 HEADTYP—Header Type Register (USB xHCI—D20:F0) 430
11.2.10 MEM_BASE_L—Memory Base Address Low Register (USB xHCI—D20:F0) 430
11.2.11 MEM_BASE_H—Memory Base Address High Register (USB xHCI—D20:F0) 430
11.2.12 SVID—USB xHCI Subsystem Vendor ID Register (USB xHCI—D20:F0) 431
11.2.13 SID—USB xHCI Subsystem ID Register (USB xHCI—D20:F0) 431
11.2.14 CAP_PTR—Capabilities Pointer Register (USB xHCI—D20:F0) 431
11.2.15 INT_LN—Interrupt Line Register (USB xHCI—D20:F0) 431
11.2.16 INT_PN—Interrupt Pin Register (USB xHCI—D20:F0) 431
11.2.17 XHCC—xHC System Bus Configuration Register (USB xHCI—D20:F0) 432
11.2.18 XHCC2—xHC System Bus Configuration Register 2 (USB xHCI—D20:F0) 432
11.2.19 SBRN—Serial Bus Release Number Register (USB xHCI—D20:F0) 432
11.2.20 FL_ADJ—Frame Length Adjustment Register (USB xHCI—D20:F0) 433
11.2.21 PWR_CAPID—PCI Power Management Capability ID Register (USB xHCI—D20:F0) 433
11.2.22 NXT_PTR1—Next Item Pointer #1 Register (USB xHCI—D20:F0) 434
11.2.23 PWR_CAP—Power Management Capabilities Register (USB xHCI—D20:F0) 434
11.2.24 PWR_CNTL_STS—Power Management Control / Status Register (USB xHCI—D20:F0) 435
11.2.25 MSI_CAPID—Message Signaled Interrupt Capability ID Register (USB xHCI—D20:F0) 435
11.2.26 NEXT_PTR2— Next Item Pointer Register #2 (USB xHCI—D20:F0) 435
11.2.27 MSI_MCTL— MSI Message Control Register (USB xHCI—D20:F0) 436
11.2.28 MSI_LMAD—MSI Lower Message Address Register (USB xHCI—D20:F0) 436
11.2.29 MSI_UMAD—MSI Upper Message Address Register (USB xHCI—D20:F0) 436
11.2.30 MSI_MD—MSI Message Data Register (USB xHCI—D20:F0) 436
11.2.31 U2OCM1 - XHCI USB2 Overcurrent Mapping Register1 (USB xHCI—D20:F0) 437
11.2.32 U2OCM2 - XHCI USB2 Overcurrent Mapping Register 2 (USB xHCI—D20:F0) 437
11.2.33 U3OCM1 - XHCI USB3 Overcurrent Pin Mapping 1 (USB xHCI—D20:F0) 438
11.2.34 U3OCM2 - XHCI USB3 Overcurrent Pin Mapping 2 (USB xHCI—D20:F0) 439
11.2.35 XUSB2PR —xHC USB 2.0 Port Routing Register (USB xHCI—D20:F0) 439
11.2.36 XUSB2PRM—xHC USB 2.0 Port Routing Mask Register (USB xHCI—D20:F0) 440
11.2.37 USB3_PSSEN—USB 3.0 Port SuperSpeed Enable Register (USB xHCI—D20:F0) 440
11.2.38 USB3PRM—USB 3.0 Port Routing Mask Register (USB xHCI—D20:F0) 441
11.2.39 USB2PDO—xHCI USB Port Disable Override Register (USB xHCI—D20:F0) 441
11.2.40 USB3PDO - USB3 Port Disable Override (USB xHCI—D20:F0) 442
11.3 Memory-Mapped I/O Registers 442
11.3.1 Host Controller Capability Registers 442
11.3.2 Host Controller Operational Registers 446
11.3.3 Host Controller Runtime Registers 462

11.3.4 Doorbell Registers 466

12 SMBus Controller Registers (D31:F3) 468

12.1 PCI Configuration Registers (SMBus—D31:F3) 468
12.1.1 VID—Vendor Identification Register (SMBus—D31:F3) 468
12.1.2 DID—Device Identification Register (SMBus—D31:F3) 468
12.1.3 PCICMD—PCI Command Register (SMBus—D31:F3) 469
12.1.4 PCISTS—PCI Status Register (SMBus—D31:F3) 469
12.1.5 RID—Revision Identification Register (SMBus—D31:F3) 470
12.1.6 PI—Programming Interface Register (SMBus—D31:F3) 470
12.1.7 SCC—Sub Class Code Register (SMBus—D31:F3) 470
12.1.8 BCC—Base Class Code Register (SMBus—D31:F3) 470
12.1.9 SMBMBAR0—D31_F3_SMBus Memory Base Address 0 Register (SMBus—D31:F3) 471
12.1.10 SMBMBAR1—D31_F3_SMBus Memory Base Address 1 Register (SMBus—D31:F3) 471
12.1.11 SMB_BASE—SMBus Base Address Register (SMBus—D31:F3) 471
12.1.12 SVID—Subsystem Vendor Identification Register (SMBus—D31:F2/F4) 471
12.1.13 SID—Subsystem Identification Register (SMBus—D31:F2/F4) 472
12.1.14 INT_LN—Interrupt Line Register (SMBus—D31:F3) 472
12.1.15 INT_PN—Interrupt Pin Register (SMBus—D31:F3) 472
12.1.16 HOSTC—Host Configuration Register (SMBus—D31:F3) 472
12.2 SMBus I/O and Memory Mapped I/O Registers 473
12.2.1 HST_STS—Host Status Register (SMBus—D31:F3) 474
12.2.2 HST_CNT—Host Control Register (SMBus—D31:F3) 475
12.2.3 HST_CMD—Host Command Register (SMBus—D31:F3) 476
12.2.4 XMIT_SLVA—Transmit Slave Address Register (SMBus—D31:F3) 477
12.2.5 HST_D0—Host Data 0 Register (SMBus—D31:F3) 477
12.2.6 HST_D1—Host Data 1 Register (SMBus—D31:F3) 477
12.2.7 Host_BLOCK_dB—Host Block Data Byte Register (SMBus—D31:F3) 478
12.2.8 PEC—Packet Error Check (PEC) Register (SMBus—D31:F3) 478
12.2.9 RCV_SLVA—Receive Slave Address Register (SMBus—D31:F3) 478
12.2.10 SLV_DATA—Receive Slave Data Register (SMBus—D31:F3) 479
12.2.11 AUX_STS—Auxiliary Status Register (SMBus—D31:F3) 479
12.2.12 AUX_CTL—Auxiliary Control Register (SMBus—D31:F3) 479
12.2.13 SMLINK_PIN_CTL—SMLink Pin Control Register (SMBus—D31:F3) 480
12.2.14 SMBus_PIN_CTL—SMBus Pin Control Register (SMBus—D31:F3) 480
12.2.15 SLV_STS—Slave Status Register (SMBus—D31:F3) 481
12.2.16 SLV_CMD—Slave Command Register (SMBus—D31:F3) 481
12.2.17 NOTIFY_DADDR—Notify Device Address Register (SMBus—D31:F3) 482
12.2.18 NOTIFY_DLOW—Notify Data Low Byte Register (SMBus—D31:F3) 482
12.2.19 NOTIFY_DHIGH—Notify Data High Byte Register (SMBus—D31:F3) 482

13 PCI Express* Configuration Registers 483

13.1 PCI Express* Configuration Registers (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 483
13.1.1 VID—Vendor Identification Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 485
13.1.2 DID—Device Identification Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 485
13.1.3 PCICMD—PCI Command Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 485
13.1.4 PCISTS—PCI Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 486
13.1.5 RID—Revision Identification Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 487
13.1.6 PI—Programming Interface Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 487
13.1.7 SCC—Sub Class Code Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 487
13.1.8 BCC—Base Class Code Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 487
13.1.9 CLS—Cache Line Size Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 487
13.1.10 PLT—Primary Latency Timer Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 488
13.1.11 HEADTYP—Header Type Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 488
13.1.12 BNUM—Bus Number Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 488
13.1.13 SLT—Secondary Latency Timer Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 488
13.1.14 IOBL—I/O Base and Limit Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 489

13.1.15 SSTS—Secondary Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 489
13.1.16 MBL—Memory Base and Limit Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 490
13.1.17 PMBL—Prefetchable Memory Base and Limit Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 490
13.1.18 PMBU32—Prefetchable Memory Base Upper 32 Bits Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 490
13.1.19 PMLU32—Prefetchable Memory Limit Upper 32 Bits Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 491
13.1.20 CAPP—Capabilities List Pointer Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 491
13.1.21 INTR—Interrupt Information Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 491
13.1.22 BCTRL—Bridge Control Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) . 492
13.1.23 CLIST—Capabilities List Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 492
13.1.24 XCAP—PCI Express* Capabilities Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 493
13.1.25 DCAP—Device Capabilities Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 493
13.1.26 DCTL—Device Control Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)... 493
13.1.27 DSTS—Device Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7).... 494
13.1.28 LCAP—Link Capabilities Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7). 495
13.1.29 LCTL—Link Control Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)..... 496
13.1.30 LSTS—Link Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)..... 497
13.1.31 SLCAP—Slot Capabilities Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 498
13.1.32 SLCTL—Slot Control Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 498
13.1.33 SLSTS—Slot Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 499
13.1.34 RCTL—Root Control Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)..... 499
13.1.35 RSTS—Root Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)..... 500
13.1.36 DCAP2—Device Capabilities 2 Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 500
13.1.37 DCTL2—Device Control 2 Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 501
13.1.38 LCTL2—Link Control 2 Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) .. 502
13.1.39 LSTS2—Link Status 2 Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) ... 503
13.1.40 MID—Message Signaled Interrupt Identifiers Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 503
13.1.41 MC—Message Signaled Interrupt Message Control Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 503
13.1.42 MA—Message Signaled Interrupt Message Address ..... Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 503
13.1.43 MD—Message Signaled Interrupt Message Data Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 504
13.1.44 SVCAP—Subsystem Vendor Capability Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 504
13.1.45 SVID—Subsystem Vendor Identification Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 504
13.1.46 PMCAP—Power Management Capability Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 504
13.1.47 PMC—PCI Power Management Capabilities Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 505
13.1.48 PMCS—PCI Power Management Control and Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 505
13.1.49 MPC2—Miscellaneous Port Configuration Register 2 (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 506
13.1.50 MPC—Miscellaneous Port Configuration Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 506
13.1.51 SMSCS—SMI/SCI Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)508
13.1.52 RPDCGEN—Root Port Dynamic Clock Gating Enable Register (PCI Express—D28:F0/F1/F2/F3/F4/F5/F6/F7) 508
13.1.53 PECR3—PCI Express* Configuration Register 3 (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 509
13.1.54 UES—Uncorrectable Error Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 509
13.1.55 UEM—Uncorrectable Error Mask Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 510

13.1.56 UEV—Uncorrectable Error Severity Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 510
13.1.57 CES—Correctable Error Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 511
13.1.58 CEM—Correctable Error Mask Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 512
13.1.59 AECC—Advanced Error Capabilities and Control Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 512
13.1.60 RES—Root Error Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 512
13.1.61 PECR2—PCI Express* Configuration Register 2 (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 513
13.1.62 PEETM—PCI Express* Extended Test Mode Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 513
13.1.63 PEC1—PCI Express* Configuration Register 1 (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 514

14 High Precision Event Timer Registers 515
14.1 Memory Mapped Registers 515
14.1.1 GCAP_ID—General Capabilities and Identification Register 516
14.1.2 GEN_CONF—General Configuration Register 517
14.1.3 GINTR_STA—General Interrupt Status Register 517
14.1.4 MAIN_CNT—Main Counter Value Register 518
14.1.5 TIMn_CONF—Timer n Configuration and Capabilities Register 518
14.1.6 TIMn_COMP—Timer n Comparator Value Register 520
14.1.7 TIMERn_PROCMSG_ROUT—Timer n Processor Message Interrupt Rout Register 521

15 Serial Peripheral Interface (SPI) 522
15.1 Serial Peripheral Interface Memory Mapped Configuration Registers 522
15.1.1 BFPR –BIOS Flash Primary Region Register (SPI Memory Mapped Configuration Registers) 523
15.1.2 HSFS—Hardware Sequencing Flash Status Register (SPI Memory Mapped Configuration Registers) 524
15.1.3 HSFC—Hardware Sequencing Flash Control Register (SPI Memory Mapped Configuration Registers) 525
15.1.4 FADDR—Flash Address Register (SPI Memory Mapped Configuration Registers) 525
15.1.5 FDATA0—Flash Data 0 Register (SPI Memory Mapped Configuration Registers) 526
15.1.6 FDATAN—Flash Data [N] Register (SPI Memory Mapped Configuration Registers) 526
15.1.7 FRAP—Flash Regions Access Permissions Register (SPI Memory Mapped Configuration Registers) 526
15.1.8 FREG0—Flash Region 0 (Flash Descriptor) Register (SPI Memory Mapped Configuration Registers) 527
15.1.9 FREG1—Flash Region 1 (BIOS Descriptor) Register (SPI Memory Mapped Configuration Registers) 527
15.1.10 FREG2—Flash Region 2 (Intel® ME) Register (SPI Memory Mapped Configuration Registers) 528
15.1.11 FREG3—Flash Region 3 (GbE) Register (SPI Memory Mapped Configuration Registers) 528
15.1.12 FREG4—Flash Region 4 (Platform Data) Register (SPI Memory Mapped Configuration Registers) 528
15.1.13 PR0—Protected Range 0 Register (SPI Memory Mapped Configuration Registers) 529
15.1.14 PR1—Protected Range 1 Register (SPI Memory Mapped Configuration Registers) 529
15.1.15 PR2—Protected Range 2 Register (SPI Memory Mapped Configuration Registers) 530
15.1.16 PR3—Protected Range 3 Register (SPI Memory Mapped Configuration Registers) 530
15.1.17 PR4—Protected Range 4 Register (SPI Memory Mapped Configuration Registers) 531
15.1.18 SSFS—Software Sequencing Flash Status Register (SPI Memory Mapped Configuration Registers) 531
15.1.19 SSFC—Software Sequencing Flash Control Register (SPI Memory Mapped Configuration Registers) 532

15.1.20 PREOP—Prefix Opcode Configuration Register (SPI Memory Mapped Configuration Registers) 533
15.1.21 OPTYPE—Opcode Type Configuration Register (SPI Memory Mapped Configuration Registers) 533
15.1.22 OPMENU—Opcode Menu Configuration Register (SPI Memory Mapped Configuration Registers) 534
15.1.23 BBAR—BIOS Base Address Configuration Register (SPI Memory Mapped Configuration Registers) 534
15.1.24 FDOC—Flash Descriptor Observability Control Register (SPI Memory Mapped Configuration Registers) 535
15.1.25 FDOD—Flash Descriptor Observability Data Register (SPI Memory Mapped Configuration Registers) 535
15.1.26 AFC—Additional Flash Control Register (SPI Memory Mapped Configuration Registers) 535
15.1.27 LVSCC— Host Lower Vendor Specific Component Capabilities Register (SPI Memory Mapped Configuration Registers) 536
15.1.28 UVSCC— Host Upper Vendor Specific Component Capabilities Register (SPI Memory Mapped Configuration Registers) 537
15.1.29 FPB—Flash Partition Boundary Register (SPI Memory Mapped Configuration Registers) 538
15.1.30 SRDL—Soft Reset Data Lock Register (SPI Memory Mapped Configuration Registers) 538
15.1.31 SRDC—Soft Reset Data Control Register (SPI Memory Mapped Configuration Registers) 538
15.1.32 SRD—Soft Reset Data Register (SPI Memory Mapped Configuration Registers) 539
15.2 Flash Descriptor Records 539
15.3 OEM Section 539
15.4 GbE SPI Flash Program Registers 539
15.4.1 GLFPR –Gigabit LAN Flash Primary Region Register (GbE LAN Memory Mapped Configuration Registers) 540
15.4.2 HSFS—Hardware Sequencing Flash Status Register (GbE LAN Memory Mapped Configuration Registers) 540
15.4.3 HSFC—Hardware Sequencing Flash Control Register (GbE LAN Memory Mapped Configuration Registers) 541
15.4.4 FADDR—Flash Address Register (GbE LAN Memory Mapped Configuration Registers) 542
15.4.5 FDATA0—Flash Data 0 Register (GbE LAN Memory Mapped Configuration Registers) 542
15.4.6 FRAP—Flash Regions Access Permissions Register (GbE LAN Memory Mapped Configuration Registers) 542
15.4.7 FREG0—Flash Region 0 (Flash Descriptor) Register (GbE LAN Memory Mapped Configuration Registers) 543
15.4.8 FREG1—Flash Region 1 (BIOS Descriptor) Register (GbE LAN Memory Mapped Configuration Registers) 543
15.4.9 FREG2—Flash Region 2 (Intel® ME) Register (GbE LAN Memory Mapped Configuration Registers) 544
15.4.10 FREG3—Flash Region 3 (GbE) Register (GbE LAN Memory Mapped Configuration Registers) 544
15.4.11 PR0—Protected Range 0 Register (GbE LAN Memory Mapped Configuration Registers) 544
15.4.12 PR1—Protected Range 1 Register (GbE LAN Memory Mapped Configuration Registers) 545
15.4.13 SSFS—Software Sequencing Flash Status Register (GbE LAN Memory Mapped Configuration Registers) 545
15.4.14 SSFC—Software Sequencing Flash Control Register (GbE LAN Memory Mapped Configuration Registers) 546
15.4.15 PREOP—Prefix Opcode Configuration Register (GbE LAN Memory Mapped Configuration Registers) 547
15.4.16 OPTYPE—Opcode Type Configuration Register (GbE LAN Memory Mapped Configuration Registers) 547
15.4.17 OPMENU—Opcode Menu Configuration Register (GbE LAN Memory Mapped Configuration Registers) 548
16 Thermal Sensor Registers (D31:F6) 549
16.1 PCI Bus Configuration Registers 549
16.1.1 VID—Vendor Identification Register 549

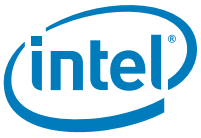
16.1.2 DID—Device Identification Register 550
16.1.3 CMD—Command Register 550
16.1.4 STS—Status Register 550
16.1.5 RID—Revision Identification Register 551
16.1.6 PI— Programming Interface Register 551
16.1.7 SCC—Sub Class Code Register 551
16.1.8 BCC—Base Class Code Register 551
16.1.9 CLS—Cache Line Size Register 551
16.1.10 LT—Latency Timer Register 551
16.1.11 HTYPE—Header Type Register 552
16.1.12 TBAR—Thermal Base Register 552
16.1.13 TBARH—Thermal Base High DWord Register 552
16.1.14 SVID—Subsystem Vendor ID Register 552
16.1.15 SID—Subsystem ID Register 553
16.1.16 CAP_PTR—Capabilities Pointer Register 553
16.1.17 INTLN—Interrupt Line Register 553
16.1.18 INTPN—Interrupt Pin Register 553
16.1.19 TBARB—BIOS Assigned Thermal Base Address Register 554
16.1.20 TBARBH—BIOS Assigned Thermal Base High DWord Register 554
16.1.21 PID—PCI Power Management Capability ID Register 554
16.1.22 PC—Power Management Capabilities Register 554
16.1.23 PCS—Power Management Control And Status Register 555
16.2 Thermal Memory Mapped Configuration Registers (Thermal Sensor – D31:F26) 555
16.2.1 TEMP—Temperature Register 556
16.2.2 TSC—Thermal Sensor Control Register 556
16.2.3 TSS—Thermal Sensor Status Register 556
16.2.4 TSEL — Thermal Sensor Enable and Lock Register 557
16.2.5 TSREL—Thermal Sensor Reporting Enable and Lock Register 557
16.2.6 TSMIC—Thermal Sensor SMI Control Register 557
16.2.7 CTT—Catastrophic Trip Point Register 558
16.2.8 TAHV—Thermal Alert High Value Register 558
16.2.9 TALV—Thermal Alert Low Value Register 558
16.2.10 TL—Throttle Levels Register 558
16.2.11 PHL—Intel® Xeon® Processor D-1500 Product Family Hot Level Register 559
16.2.12 PHLC—PHL Control Register 559
16.2.13 TAS — Thermal Alert Status Register 559
16.2.14 TSPIEN — PCI Interrupt Event Enables Register 560
16.2.15 TSGPEN—General Purpose Event Enables Register 560

17 Intel® Management Engine Subsystem Registers (D22:F[3:0]) 561

17.1 First Intel® Management Engine Interface (Intel® MEI) Configuration Registers (Intel® MEI 1 — D22:F0) 561
17.1.1 PCI Configuration Registers (Intel® MEI 1—D22:F0) 561
17.1.2 MEI0_MBAR—Intel® MEI 1 MMIO Registers 571
17.2 Second Intel® Management Engine Interface (Intel® MEI 2) Configuration Registers (Intel® MEI 2—D22:F1) 573
17.2.1 PCI Configuration Registers (Intel® MEI 2—D22:F2) 573
17.2.2 MEI1_MBAR—Intel® MEI 2 MMIO Registers 580
17.3 IDE Redirect IDER Registers (IDER — D22:F2) 582
17.3.1 PCI Configuration Registers (IDER—D22:F2) 582
17.3.2 IDER BAR0 Registers 589
17.3.3 IDER BAR1 Registers 597
17.3.4 IDER BAR4 Registers 598
17.4 Serial Port for Remote Keyboard and Text (KT) Redirection (KT — D22:F3) 603
17.4.1 PCI Configuration Registers (KT — D22:F3) 603
17.4.2 KT IO/Memory Mapped Device Registers 608

Figures

3-1 Generation of SERR# to Platform 53
3-2 LPC Interface Diagram 63
3-3 Intel® Xeon® Processor D-1500 Product Family DMA Controller 67
3-4 DMA Request Assertion through LDRQ# 71



3-5 Conceptual Diagram of SLP_LAN# 108
3-6 TCO Legacy/Compatible Mode SMBus Configuration 114
3-7 Serial Post over GPIO Reference Circuit 117
3-8 Flow for Port Enable / Device Present Bits 124
3-9 Serial Data transmitted over the SGPIO Interface 128
3-10 EHCI with USB 2.0 with Rate Matching Hub 143
3-11 Intel® Xeon® Processor D-1500 Product Family Intel® Management Engine (Intel® ME) High-Level Block Diagram 166
3-12 Flash Descriptor Sections 170

Tables

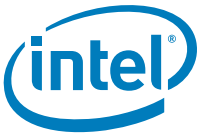
1-1 Industry Specifications 24
1-2 Intel® Xeon® Processor D-1500 Product Family Integrated 32
1-3 Intel® Xeon® Processor D-1500 Product Family Device and Revision ID 32
2-1 SoC Clock Inputs 36
2-2 Clock Outputs 36
2-3 Intel® Xeon® Processor D-1500 Product Family PLLs 37
2-4 Modulator Blocks 37
2-5 ICC Registers under Intel® Management Engine (Intel® ME) Control 38
3-1 PCI Express* Ports 1 Through 4 - Supported Configurations 50
3-2 PCI Express Ports 5 Through 8 - Supported Configurations 50
3-3 MSI versus PCI IRQ Actions 50
3-4 LAN Mode Support 58
3-5 LPC Cycle Types Supported 63
3-6 Start Field Bit Definitions 64
3-7 Cycle Type Bit Definitions 64
3-8 Transfer Size Bit Definition 64
3-9 SYNC Bit Definition 65
3-10 DMA Transfer Size 69
3-11 Address Shifting in 16-Bit I/O DMA Transfers 69
3-12 Counter Operating Modes 75
3-13 Interrupt Controller Connections 77
3-14 Interrupt Status Registers 78
3-15 Content of Interrupt Vector Byte 78
3-16 APIC Interrupt Mapping1 84
3-17 Stop Frame Explanation 87
3-18 Data Frame Format 87
3-19 Configuration Bits Reset by RTCRST# Assertion 90
3-20 General Power States for Systems Using Intel® Xeon® Processor D-1500 Product Family 92
3-21 State Transition Rules for Intel® Xeon® Processor D-1500 Product Family 92
3-22 System Power Plane 93
3-23 Causes of SMI and SCI 94
3-24 Sleep Types 97
3-25 Causes of Wake Events 98
3-26 GPI Wake Events 99
3-27 Transitions Due to Power Failure 100
3-28 Transitions Due to Power Button 100
3-29 Transitions Due to RI# Signal 101
3-30 Write Only Registers with Read Paths in ALT Access Mode 104
3-31 PIC Reserved Bits Return Values 105
3-32 Register Write Accesses in ALT Access Mode 106
3-33 SUSPWRDNACK / SUSWARN# / GPIO30 Pin Behavior 109
3-34 SUSPWRDNACK during Reset 109
3-35 Causes of Host and Global Resets 111
3-36 Event Transitions that Cause Messages 114
3-37 Multi-activity LED Message Type 127
3-38 Legacy Replacement Routing 129
3-39 Debug Port Behavior 138
3-40 I^2C* Block Read 148
3-41 Enable for SMBALERT# 150
3-42 Enables for SMBus Slave Write and SMBus Host Events 151
3-43 Enables for the Host Notify Command 151
3-44 Slave Write Registers 152

3-45 Command Types 153
3-46 Slave Read Cycle Format 153
3-47 Data Values for Slave Read Registers 154
3-48 Host Notify Format 156
3-49 Intel® Xeon® Processor D-1500 Product Family Thermal Throttle States (T-states) 159
3-50 Intel® Xeon® Processor D-1500 Product Family Thermal Throttling Configuration Registers 159
3-51 Region Size versus Erase Granularity of Flash Components 169
3-52 Region Access Control Table 171
3-53 Hardware Sequencing Commands and Opcode Requirements 174
3-54 Flash Protection Mechanism Summary 176
3-55 Recommended Pinout for 8-Pin Serial Flash Device 177
3-56 Recommended Pinout for 16-Pin Serial Flash Device 177
4-1 PCI Devices and Functions 182
4-2 Fixed I/O Ranges Decoded by Intel® Xeon® Processor D-1500 Product Family 183
4-3 Variable I/O Decode Ranges 185
4-4 Memory Decode Ranges from Processor Perspective 186
4-5 SPI Mode Address Swapping 188
5-1 Chipset Configuration Register Memory Map (Memory Space) 190
5-2 Thermal Initialization Registers 223
6-1 Gigabit LAN Configuration Registers Address Map (Gigabit LAN—D25:F0) 225
6-2 Gigabit LAN Capabilities and Status Registers Address Map (Gigabit LAN—MBARA) 236
7-1 LPC Interface PCI Register Address Map (LPC I/F—D31:F0) 240
7-2 DMA Registers 259
7-3 PIC Registers 268
7-4 APIC Direct Registers 274
7-5 APIC Indirect Registers 275
7-6 RTC I/O Registers 279
7-7 RTC (Standard) RAM Bank 279
7-8 Processor Interface PCI Register Address Map 282
7-9 Power Management PCI Register Address Map (PM—D31:F0) 284
7-10 APM Register Map 292
7-11 ACPI and Legacy I/O Register Map 293
7-12 TCO I/O Register Address Map 307
7-13 Registers to Control GPIO Address Map 313
8-1 SATA Controller PCI Register Address Map (SATA–D31:F2) 325
8-2 Bus Master IDE I/O Register Address Map 347
8-3 AHCI Register Address Map 354
8-4 Generic Host Controller Register Address Map 354
8-5 Port [5:0] DMA Register Address Map 359
9-1 SATA Controller PCI Register Address Map (SATA–D31:F5) 373
9-2 Bus Master IDE I/O Register Address Map 386
10-1 USB EHCI PCI Register Address Map (USB EHCI—D29:F0) 393
10-2 Enhanced Host Controller Capability Registers 410
10-3 Enhanced Host Controller Operational Register Address Map 412
10-4 Debug Port Register Address Map 423
11-1 USB xHCI PCI Register Address Map (USB xHCI—D20:F0) 426
11-2 Enhanced Host Controller Capability Registers 442
11-3 Enhanced Host Controller Operational Register Address Map 446
11-4 Enhanced Host Controller Operational Register Address Map 462
12-1 SMBus Controller PCI Register Address Map (SMBus—D31:F3) 468
12-2 SMBus I/O and Memory Mapped I/O Register Address Map 473
13-1 PCI Express* Configuration Registers Address Map (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) 483
14-1 Memory-Mapped Register Address Map 515
15-1 Serial Peripheral Interface (SPI) Register Address Map (SPI Memory Mapped Configuration Registers) 522
15-2 Gigabit LAN SPI Flash Program Register Address Map (GbE LAN Memory Mapped Configuration Registers) 539
16-1 Thermal Sensor Register Address Map 549
16-2 Thermal Memory Mapped Configuration Register Address Map 555
17-1 Intel® MEI 1 Configuration Registers Address Map (Intel® MEI 1—D22:F0) 561
17-2 Intel® MEI 1 MMIO Register Address Map 571
17-3 Intel® MEI 2 Configuration Registers Address Map (Intel® MEI 2—D22:F1) 573
17-4 Intel® MEI 2 MMIO Register Address Map 580
17-5 IDE Redirect Function IDER Register Address Map 582

17-6 IDER BAR0 Register Address Map 589
17-7 IDER BAR1 Register Address Map 597
17-8 IDER BAR4 Register Address Map 598
17-9 Serial Port for Remote Keyboard and Text (KT) Redirection Register Address Map 603
17-10 KT IO/Memory Mapped Device Register Address Map 608

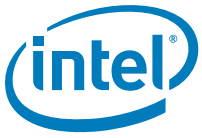
Revision History

Revision Number	Description	Revision Date
001	• Initial Release.	March 2015
002	• Updated Section 3.13.2.2, Advanced TCO Mode • Deleted Figure 3-7 Advanced TCO Mode • Added GPI_NMI_EN_2 and GPI_NMI_EN_3 registers • Added GPI_NMI_STS_2 and GPI_NMI _STS_3 registers • Updated STS bit[15] to reserved in Section 16.1.4.	November 2015
003	• Changed i127LM/V to i217LM/V.	April 2021



Platform Controller Hub Features

- PCI Express*
  - Up to eight PCI Express root ports
  - Supports PCI Express Rev 2.0 running at up to 5.0 GT/s
  - Ports 1-4 and 5-8 can independently be configured to support multiple port configurations
  - Module based Hot-Plug supported (that is, ExpressCard*)
  - NEW: Latency Tolerance Reporting
  - NEW: Optimized Buffer Flush/Fill
- Integrated Serial ATA Host Controller
  - Up to six SATA ports
  - Data transfer rates supported: 6.0 Gb/s, 3.0 Gb/s, and 1.5 Gb/s on all ports
  - Integrated AHCI controller
- Eight TACH signals and one PWM signal
- Platform Environmental Control Interface (PECI) and Simple Serial Transport (SST) 1.0 Bus
- Integrated Clock Controller
  - Full featured platform clocking without need for a discrete clock chip
  - Eight PCIe* 2.0 specification compliant clocks, four PCIe 3.0 specification compliant clocks, five 33 MHz PCI clocks, and two Flex Clocks that can be configured for various frequencies
- System TCO Reduction Circuits
  - Timers to generate SMI# and Reset upon detection of system hang
  - Timers to detect improper processor reset
  - Supports ability to disable external devices
- JTAG
  - Boundary Scan for testing during board manufacturing
- External Glue Integration
  - Integrated Pull-down and Series resistors on USB
- Enhanced DMA Controller
  - Two cascaded 8237 DMA controllers
  - Supports LPC DMA
- Firmware Hub I/F supports BIOS Memory size up to 8 MB
- Low Pin Count (LPC) I/F
  - Supports two Master/DMA devices.
  - Support for Security Device (Trusted Platform Module) connected to LPC
- Interrupt Controller
  - Supports up to eight legacy interrupt pins
  - Supports PCI 2.3 Message Signaled Interrupts
  - Two cascaded 8259 with 15 interrupts
  - Integrated I/O APIC capability with 24 interrupts
  - Supports Processor System Bus interrupt delivery
- USB
  - xHCI Host Controller, supports up to four SuperSpeed USB 3.0 connections and four USB 2.0 connections
  - More flexibility in pairing USB 3.0 and USB 2.0 signals to the same connector
  - One EHCI Host Controller, supporting up to four external USB 2.0 ports
  - Support for dynamic power gating and Intel® Power Management Framework (PMF)
  - Per-Port-Disable Capability
  - Includes one USB 2.0 High-speed Debug Ports
  - Supports wake-up from sleeping states S1-S4
- Integrated Gigabit LAN Controller
  - Connection utilizes PCI Express pins
  - Integrated ASF Management Controller
  - Network security with System Defense
  - Supports IEEE 802.3
  - 10/100/1000 Mbps Ethernet Support
  - Jumbo Frame Support
- Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d) Support
- Intel® Trusted Execution Technology (Intel® TXT) Support
- Power Management Logic
  - Supports ACPI 4.0a
  - ACPI-defined power states (processor driven C states)
  - ACPI Power Management Timer
  - SMI# generation
  - All registers readable/restorable for proper resume from 0 V core well suspend states
  - Support for APM-based legacy power management for non-ACPI implementations
- Serial Peripheral Interface (SPI)
  - Supports up to two SPI devices
  - Supports 20 MHz, 33 MHz, and 50 MHz SPI devices
  - NEW: Supports Quad I/O Fast Read, Quad Output Fast Read, Dual I/O Fast Read
  - NEW: Support for TPM over SPI with the addition of SPI_CS2# chip select pin
  - NEW: Supports Serial Flash Discoverable Parameter (SFDP)
  - Support up to two different erase granularities
- SMBus
  - Interface speeds of up to 100 kbps
  - Supports SMBus 2.0 Specification
  - Host interface allows processor to communicate using SMBus
  - Slave interface allows an internal or external microcontroller to access system resources
  - Supports most two-wire components that are also I^2C* compatible



- 1.05 V operation with tolerance up to 3.3 V I/O
- 1.05 V Core Voltage
- Integrated Voltage Regulators for select power rails
- GPIO
  - — Open-Drain, Inversion
  - — GPIO lock down
- SMLink
  - — Provides independent manageability bus through SMLink0 and SMLink1
  - — SMLink0 dedicated to EC or BMC, operating up to 100 kHz
- High Precision Event Timers
  - — Advanced operating system interrupt scheduling
- Timers Based on 8254
  - — System timer, Refresh request, Speaker tone output
- Real-Time Clock
  - — 256 byte battery-backed CMOS RAM
  - — Integrated oscillator components
  - — Lower Power DC/DC Converter implementation

§

1 Introduction

1.1 About This Manual

This document is intended for Original Equipment Manufacturers and BIOS vendors creating products based on the Integrated Intel® Xeon® Processor D-1500 Product Family Logic Platform Controller Hub. See Section 1.3 for definitions and supported features).

Note: Throughout this document, Intel® Xeon® Processor D-1500 Product Family is used as a general term and refers to all Intel® Xeon® Processor D-1500 Product Family Integrated Logic Platform Controller Hub, unless specifically noted otherwise.

This manual assumes a working knowledge of the vocabulary and principles of PCI Express*, USB, AHCI, SATA, SMBus, ACPI and Low Pin Count (LPC). Although some details of these features are described within this manual, refer to the individual industry specifications listed in Table 1-1 for the complete details.

All PCI buses, devices and functions in this manual are abbreviated using the following nomenclature; Bus:Device:Function. This manual abbreviates buses as B*n*, devices as D*n* and functions as F*n*. For example Device 31 Function 0 is abbreviated as D31:F0, Bus 1 Device 8 Function 0 is abbreviated as B1:D8:F0. Generally, the bus number will not be used, and can be considered to be Bus 0.

Table 1-1. Industry Specifications (Sheet 1 of 2)

Specification	Location
PCI Express Base Specification*, Revision 2.0	http://www.pcisig.com/specifications
Low Pin Count Interface Specification, Revision 1.1 (LPC)	http://developer.intel.com/design/chipsets/industry/lpc.htm
System Management Bus Specification, Version 2.0 (SMBus)	http://www.smbus.org/specs/
PCI Local Bus Specification, Revision 2.3 (PCI)	http://www.pcisig.com/specifications
PCI Power Management Specification, Revision 1.2	http://www.pcisig.com/specifications
Universal Serial Bus Specification (USB), Revision 2.0	http://www.usb.org/developers/docs
Advanced Configuration and Power Interface, Version 4.0a (ACPI)	http://www.acpi.info/spec.htm
Enhanced Host Controller Interface Specification for Universal Serial Bus, Revision 1.0 (EHCI)	http://developer.intel.com/technology/usb/ehcispec.htm
eXtensible Host Controller Interface for Universal Serial Bus (xHCI), Revision 1.0	http://www.intel.com/technology/usb/xhcispec.htm
Serial ATA Specification, Revision 3.0	http://www.serialata.org/
Serial ATA II: Extensions to Serial ATA 1.0, Revision 1.0	http://www.serialata.org
Serial ATA II Cables and Connectors Volume 2 Gold	http://www.serialata.org
Alert Standard Format Specification, Version 1.03	http://www.dmtf.org/standards/asf
IEEE 802.3 Fast Ethernet*	http://standards.ieee.org/getieee802/
AT Attachment - 6 with Packet Interface (ATA/ATAPI - 6)	http://T13.org (T13 1410D)
IA-PC HPET (High Precision Event Timers) Specification, Revision 1,0a	http://www.intel.com/hardwaredesign/hpetspec_1.pdf
Trusted Platform Module (TPM) Specification 1.3 Note: TPM over SPI supports 8 bytes transactions max.	http://www.trustedcomputinggroup.org/specs/TPM

Table 1-1. Industry Specifications (Sheet 2 of 2)

Specification	Location
Intel® Virtualization Technology	http://www.intel.com/technology/virtualization/index.htm
SFF-8485 Specification for Serial GPIO (SGPIO) Bus, Revision 0.7	http://www.intel.com/technology/virtualization/index.htm
Advanced Host Controller Interface specification for Serial ATA, Revision 1.3	http://www.intel.com/technology/serialata/ahci.htm

1.1.1 Chapter Descriptions

Chapter 1, "Introduction" introduces Intel® Xeon® Processor D-1500 Product Family, provides information on the organization of the manual and gives a general overview of Intel® Xeon® Processor D-1500 Product Family.

Chapter 2, "Intel® Xeon® Processor D-1500 Product Family and System Clocks" provides a list of each clock domain associated with Intel® Xeon® Processor D-1500 Product Family.

Chapter 3, "Functional Description" provides a detailed description of the functions in Intel® Xeon® Processor D-1500 Product Family.

Chapter 4, "Register and Memory Mapping" provides an overview of the registers, fixed I/O ranges, variable I/O ranges and memory ranges decoded by Intel® Xeon® Processor D-1500 Product Family.

Chapter 5, "Chipset Configuration Registers" provides a detailed description of registers and base functionality that is related to chipset configuration. It contains the root complex register block, which describes the behavior of the upstream internal link.

Chapter 6, "Gigabit LAN Configuration Registers" provides a detailed description of registers that reside in Intel® Xeon® Processor D-1500 Product Family's integrated LAN controller. The integrated LAN Controller resides at Device 25, Function 0 (D25:F0).

Chapter 7, "LPC Interface Bridge Registers (D31:F0)" provides a detailed description of registers that reside in the LPC bridge. This bridge resides at Device 31, Function 0 (D31:F0). This function contains registers for many different units within Intel® Xeon® Processor D-1500 Product Family including DMA, Timers, Interrupts, Processor Interface, GPIO, Power Management, System Management and RTC.

Chapter 8, "SATA Controller Registers (D31:F2)" provides a detailed description of registers that reside in the SATA controller #1. This controller resides at Device 31, Function 2 (D31:F2).

Chapter 9, "PCI Configuration Registers (SATA–D31:F5)" provides a detailed description of registers that reside in the SATA controller #2. This controller resides at Device 31, Function 5 (D31:F5).

Chapter 10, "EHCI Controller Registers (D29:F0)" provides a detailed description of registers that reside in the two EHCI host controllers. These controllers reside at Device 29, Function 0 (D29:F0) and Device 26, Function 0 (D26:F0).

Chapter 11, "xHCI Controller Registers (D20:F0)" provides a detailed description of registers that reside in the xHCI. This controller resides at Device 20, Function 0 (D20:F0).

Chapter 12, "SMBus Controller Registers (D31:F3)" provides a detailed description of registers that reside in the SMBus controller. This controller resides at Device 31, Function 3 (D31:F3).

Chapter 13, "PCI Express* Configuration Registers" provides a detailed description of registers that reside in the PCI Express controller. This controller resides at Device 28, Functions 0 to 7 (D28:F0-F7).

Chapter 14, "High Precision Event Timer Registers" provides a detailed description of registers that reside in the multimedia timer memory mapped register space.

Chapter 15, "Serial Peripheral Interface (SPI)" provides a detailed description of registers that reside in the SPI memory mapped register space.

Chapter 16, "Thermal Sensor Registers (D31:F6)" provides a detailed description of registers that reside in the thermal sensors PCI configuration space. The registers reside at Device 31, Function 6 (D31:F6).

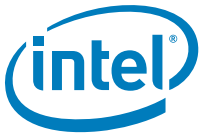
Chapter 17, "Intel® Management Engine Subsystem Registers (D22:F[3:0])" provides a detailed description of registers that reside in the Intel® Management Engine (Intel® ME) controller. The registers reside at Device 22, Function 0 (D22:F0).

1.2 Overview

Intel® Xeon® Processor D-1500 Product Family provides extensive I/O support. Functions and capabilities include:

- *PCI Express* Base Specification,* Revision 2.0 support for up to eight ports with transfers up to 5 GT/s
- ACPI Power Management Logic Support, Revision 4.0a
- Enhanced DMA controller, interrupt controller, and timer functions
- Integrated Serial ATA host controllers with independent DMA operation on up to six ports
- xHCI USB controller provides support for up to 4 USB ports, of which four can be configured as SuperSpeed USB 3.0 ports.
- One legacy EHCI USB controller provides a USB debug port.
- Integrated 10/100/1000 Gigabit Ethernet MAC with System Defense
- *System Management Bus (SMBus) Specification*, Version 2.0 with additional support for I^2C* devices
- Supports Intel® Virtualization Technology for Directed I/O (Intel® VT-d)
- Supports Intel® Trusted Execution Technology (Intel® TXT)
- Integrated Clock Controller
- Low Pin Count (LPC) interface
- Firmware Hub (FWH) interface support
- Serial Peripheral Interface (SPI) support
- JTAG Boundary Scan support

Note: See Section 1.3 for details on feature availability.



1.2.1 Capability Overview

The following sub-sections provide an overview of Intel® Xeon® Processor D-1500 Product Family's capabilities.

PCI Express* Interface

Intel® Xeon® Processor D-1500 Product Family provides up to 8 PCI Express Root Ports, supporting the *PCI Express Base Specification,* Revision 2.0. Each Root Port x1 lane supports up to 5 Gb/s bandwidth in each direction (10 GB/s concurrent). PCI Express Root Ports 1–4 or Ports 5–8 can independently be configured to support multiple port width configurations. See Section 1.3 for details on feature availability.

Serial ATA (SATA) Controller

Intel® Xeon® Processor D-1500 Product Family has two integrated SATA host controllers that support independent DMA operation on up to six ports and support data transfer rates of up to 6.0 GB/s on all ports. The SATA controller contains two modes of operation – a legacy mode using I/O space, and an AHCI mode using memory space. Software that uses legacy mode will not have AHCI capabilities.

Intel® Xeon® Processor D-1500 Product Family supports the Serial ATA Specification, Revision 3.0. Intel® Xeon® Processor D-1500 Product Family also supports several optional sections of the Serial ATA II: Extensions to Serial ATA 1.0 Specification, Revision 1.0 (AHCI support is required for some elements).

See Section 1.3 for details on feature availability.

AHCI

Intel® Xeon® Processor D-1500 Product Family provides hardware support for Advanced Host Controller Interface (AHCI), a standardized programming interface for SATA host controllers. Platforms supporting AHCI may take advantage of performance features such as no master/slave designation for SATA devices – each device is treated as a master – and hardware-assisted native command queuing. AHCI also provides usability enhancements, such as Hot-Plug. AHCI requires appropriate software support (such as, an AHCI driver) and for some features, hardware support in the SATA device or additional platform hardware. See Section 1.3 for details on feature availability.

Low Pin Count (LPC) Interface

Intel® Xeon® Processor D-1500 Product Family implements an LPC Interface as described in the *LPC 1.1 Specification*. The Low Pin Count (LPC) bridge function of Intel® Xeon® Processor D-1500 Product Family is mapped as PCI D31:F0 and supports a memory size up to 8 MB, two master/DMA devices, interrupt controllers, timers, power management, system management, Super I/O, and RTC.

Serial Peripheral Interface (SPI)

In addition to the standard Dual Output Fast Read mode, the SPI interface in Intel® Xeon® Processor D-1500 Product Family supports new Dual I/O Fast Read, Quad I/O Fast Read and Quad Output Fast Read. To enable the new Quad I/O operation modes, all data transfer signals in the interface are bidirectional and two new signals (SPI_IO2 and SPI_IO3) have been added to the basic four-wire interface: Clock, Master Out Slave In (MOSI), Master In Slave Out (MISO) and active-low chip selects (CS#). Intel® Xeon® Processor D-1500 Product Family supports three chip selects: SPI_CS0# and

SPI_CS1# are used to access two separate SPI Flash components in Descriptor Mode. SPI_CS2# is dedicated only to support Trusted Platform Module (TPM) on SPI (TPM can be configured through Intel® Xeon® Processor D-1500 Product Family soft straps to operate over LPC or SPI, but no more than 1 TPM is allowed in the system). SPI_CS2# may not be used for any purpose other than TPM.

The SPI Flash Controller supports running instructions at 20 MHz, 33 MHz, and 50 MHz, and can be used by Intel® Xeon® Processor D-1500 Product Family for BIOS code, to provide chipset configuration settings, internal micro-processor code, and integrated Gigabit Ethernet MAC/PHY configuration. The SPI Flash Controller supports the Serial Flash Discoverable Parameter (SFDP) JEDEC standard that provides a consistent way of describing the functional and feature capabilities of serial flash devices in a standard set of internal parameter tables. The SPI Flash Controller queries these parameter tables to discover the attributes to enable divergent features from multiple SPI part vendors, such as Quad I/O Fast Read capabilities or device storage capacity, among others.

Compatibility Modules (DMA Controller, Timer/Counters, Interrupt Controller)

The DMA controller incorporates the logic of two 8237 DMA controllers, with seven independently programmable channels. Channels 0–3 are hardwired to 8-bit, count-by-byte transfers, and channels 5–7 are hardwired to 16-bit, count-by-word transfers. Any two of the seven DMA channels can be programmed to support fast Type-F transfers. Channel 4 is reserved as a generic bus master request.

Intel® Xeon® Processor D-1500 Product Family supports LPC DMA, which is similar to ISA DMA, through Intel® Xeon® Processor D-1500 Product Family DMA controller. LPC DMA is handled through the use of the LDRQ# lines from peripherals and special encoding on LAD[3:0] from the host. Single, Demand, Verify, and Increment modes are supported on the LPC interface.

The timer/counter block contains three counters that are equivalent in function to those found in one 8254 programmable interval timer. These three counters are combined to provide the system timer function, and speaker tone. The 14.318 MHz oscillator input provides the clock source for these three counters.

Intel® Xeon® Processor D-1500 Product Family provides an ISA-compatible Programmable Interrupt Controller (PIC) that incorporates the functionality of two 8259 interrupt controllers. The two interrupt controllers are cascaded so that 14 external and two internal interrupts are possible. In addition, Intel® Xeon® Processor D-1500 Product Family supports a serial interrupt scheme.

All of the registers in these modules can be read and restored. This is required to save and restore system state after power has been removed and restored to the platform.

Advanced Programmable Interrupt Controller (APIC)

In addition to the standard ISA-compatible Programmable Interrupt controller (PIC) described in the previous section, Intel® Xeon® Processor D-1500 Product Family incorporates the Advanced Programmable Interrupt Controller (APIC).

Universal Serial Bus (USB) Controllers

Intel® Xeon® Processor D-1500 Product Family contains one eXtensible Host Controller Interface (xHCI) controller and one Enhanced Host Controller Interface (EHCI) controllers. The xHCI controller is mapped as PCI D20:F0 and it supports up to 4 USB 2.0 ports of which all 4 can be configured as SuperSpeed (USB 3.0) ports.

EHCI controller 1 (EHCI1) is located at D29:F0 and it supports up to 4 USB 2.0 ports. One of the USB 2.0 ports in the EHCI controller can be used for a Debug Port (not available through xHCI). 1.

See Section 1.3 for details on feature availability.

Gigabit Ethernet Controller

The Gigabit Ethernet Controller provides a system interface using a PCI function. The controller provides a full memory-mapped or I/O mapped interface along with a 64-bit address master support for systems using more than 4 GB of physical memory and DMA (Direct Memory Addressing) mechanisms for high performance data transfers. Its bus master capabilities enable the component to process high-level commands and perform multiple operations. This lowers processor utilization by off-loading communication tasks from the processor. Two large configurable transmit and receive FIFOs (up to 20 KB each) help prevent data underruns and overruns while waiting for bus accesses. This enables the integrated LAN controller to transmit data with minimum interframe spacing (IFS).

The LAN controller can operate at multiple speeds (10/100/1000 MB/s) and in either full duplex or half duplex mode. In full duplex mode the LAN controller adheres with the *IEEE 802.3x Flow Control* Specification. Half duplex performance is enhanced by a proprietary collision reduction mechanism. See Section 3.3 for details.

RTC

Intel® Xeon® Processor D-1500 Product Family contains a Motorola MC146818B-compatible real-time clock with 256 bytes of battery-backed RAM. The real-time clock performs two key functions – keeping track of the time of day and storing system data, even when the system is powered down. The RTC operates on a 32.768-kHz crystal and a 3-V battery.

The RTC also supports two lockable memory ranges. By setting bits in the configuration space, two 8-byte ranges can be locked to read and write accesses. This prevents unauthorized reading of passwords or other system security information.

The RTC also supports a date alarm that allows for scheduling a wake up event up to 30 days in advance, rather than just 24 hours in advance.

GPIO

Various general purpose inputs and outputs are provided for custom system design. The number of inputs and outputs varies depending on Intel® Xeon® Processor D-1500 Product Family configuration.

Enhanced Power Management

Intel® Xeon® Processor D-1500 Product Family's power management functions fully support the *Advanced Configuration and Power Interface (ACPI) Specification,* Revision 4.0a, and include enhanced clock control and various low-power (suspend) states (such as Suspend-to-RAM and Suspend-to-Disk). A hardware-based thermal management circuit permits software-independent entrance to low-power states.

Manageability

Intel® Xeon® Processor D-1500 Product Family integrates several functions designed to manage the system and lower the total cost of ownership (TCO) of the system. These system management functions are designed to report errors, diagnose the system, and recover from system lockups without the aid of an external microcontroller.

- **TCO Timer.** Intel® Xeon® Processor D-1500 Product Family's integrated programmable TCO timer is used to detect system locks. The first expiration of the timer generates an SMI# that the system can use to recover from a software lock. The second expiration of the timer causes a system reset to recover from a hardware lock.
- **Processor Present Indicator.** Intel® Xeon® Processor D-1500 Product Family looks for the processor to fetch the first instruction after reset. If the processor does not fetch the first instruction, Intel® Xeon® Processor D-1500 Product Family will reboot the system.
- **ECC Error Reporting.** When detecting an ECC error, the host controller has the ability to send one of several messages to Intel® Xeon® Processor D-1500 Product Family. The host controller can instruct Intel® Xeon® Processor D-1500 Product Family to generate either an SMI#, NMI, SERR#, or TCO interrupt.
- **Function Disable.** Intel® Xeon® Processor D-1500 Product Family provides the ability to disable the following integrated functions: LAN, USB, LPC, SATA, PCI Express* or SMBus. Once disabled, these functions no longer decode I/O, memory, or PCI configuration space. Also, no interrupts or power management events are generated from the disabled functions.
- **Intruder Detect.** Intel® Xeon® Processor D-1500 Product Family provides an input signal (INTRUDER#) that can be used to inform the system in the event of the case being opened. Intel® Xeon® Processor D-1500 Product Family can be programmed to generate an SMI# or TCO interrupt due to an active INTRUDER# signal.

System Management Bus (SMBus 2.0)

Intel® Xeon® Processor D-1500 Product Family contains an SMBus Host interface that allows the processor to communicate with SMBus slaves. This interface is compatible with most I^2C devices. Special I^2C commands are implemented.

Intel® Xeon® Processor D-1500 Product Family SMBus host controller provides a mechanism for the processor to initiate communications with SMBus peripherals (slaves). Also, Intel® Xeon® Processor D-1500 Product Family supports slave functionality, including the Host Notify protocol. Hence, the host controller supports eight command protocols of the SMBus interface (see *System Management Bus (SMBus) Specification,* version 2.0): Quick Command, Send Byte, Receive Byte, Write Byte/Word, Read Byte/Word, Process Call, Block Read/Write, and Host Notify.

Intel® Xeon® Processor D-1500 Product Family SMBus also implements hardware-based Packet Error Checking for data robustness and the Address Resolution Protocol (ARP) to dynamically provide addresses to all SMBus devices.

Intel® Virtualization Technology for Directed I/O (Intel® VT-d)

Intel® Xeon® Processor D-1500 Product Family provides hardware support for implementation of Intel® Virtualization Technology with Directed I/O (Intel® VT-d). Intel® VT-d consists of technology components that support the virtualization of platforms based on Intel Architecture processors. Intel® VT-d enables multiple operating systems and applications to run in independent partitions. A partition behaves like a virtual machine (VM) and provides isolation and protection across partitions. Each partition is allocated its own subset of host physical memory.

JTAG Boundary-Scan

Intel® Xeon® Processor D-1500 Product Family implements the industry standard JTAG interface and enables Boundary-Scan. Boundary-Scan can be used to ensure device connectivity during the board manufacturing process. The JTAG interface allows system manufacturers to improve efficiency by using industry available tools to test Intel® Xeon® Processor D-1500 Product Family on an assembled board. Since JTAG is a serial interface, it eliminates the need to create probe points for every pin in an XOR chain. This eases pin breakout and trace routing and simplifies the interface between the system and a bed-of-nails tester.

Note: The TRST# JTAG signal is an optional signal in the IEEE* 1149 JTAG Specification and is not implemented in Intel® Xeon® Processor D-1500 Product Family.

Integrated Clock Controller

Intel® Xeon® Processor D-1500 Product Family contains an Integrated Clock Controller (ICC) that generates various platform clocks from a 25 MHz crystal source. The ICC contains PLLs, Modulators, and Dividers for generating various clocks suited to the platform needs. The ICC supplies up to eight 100 MHz PCI Express 2.0 Specification compliant clocks, one 100 MHz PCI Express* 3.0 Specification compliant clock for BCLK, two 100 MHz PCI Express 3.0 Specification compliant clocks for PEG slots, one 100 MHz PCI Express 3.0 Specification compliant clock for Intel® In-Target Probe (Intel® ITP) or a third PEG slot five 33 MHz PCI 2.3 Local Bus Specification compliant single-ended clocks for LPC/TPM devices and two Flex Clocks that can be configured to various frequencies that include 14.318 MHz, 33 MHz, and 24/48 MHz for use with SIO, TPM, EC, LPC, and any other legacy functions.

Serial Over LAN (SOL) Function

This function supports redirection of keyboard and text screens to a terminal window on a remote console. The keyboard and text redirection enables the control of the client machine through the network without the need to be physically near that machine. Text and keyboard redirection allows the remote machine to control and configure a client system. The SOL function emulates a standard PCI device and redirects the data from the serial port to the management console using the integrated LAN.

Intel® KVM Technology

Intel® KVM technology provides enhanced capabilities to its predecessor – SOL. In addition to the features set provided by SOL, Intel® KVM technology provides mouse and graphic redirection across the integrated LAN. Unlike SOL, Intel® KVM technology

does not appear as a host accessible PCI device, but is instead almost completely performed by Firmware with minimal BIOS interaction. The Intel® KVM technology feature is only available with internal graphics.

IDE-R Function

The IDE-R function is an IDE Redirection interface that provides client connection to management console ATA/ATAPI devices, such as hard disk drives and optical disk drives. A remote machine can setup a diagnostic software or operating system installation image and direct the client to boot an IDE-R session. The IDE-R interface is the same as the IDE interface; although, the device is not physically connected to the system and supports the ATA/ATAPI-6 specification. IDE-R does not conflict with any other type of boot and can, instead, be implemented as a boot device option. The device attached through IDE-R is only visible to software during a management boot session. During normal boot session, the IDE-R controller does not appear as a PCI present device.

1.3 Intel® Xeon® Processor D-1500 Product Family Integrated Chipset Definition

Table 1-2. Intel® Xeon® Processor D-1500 Product Family Integrated

Feature Set	BDE Integrated Chipset
PCI Express* 2.0 Ports	8
Total number of USB ports: • USB 3.0 Capable Ports (SuperSpeed and all USB 2.0 speeds) • USB 2.0 Only Ports	8 4 4
Total number of SATA ports: • SATA Ports (6 Gb/s, 3 Gb/s, and 1.5 Gb/s) • SATA Ports (3 Gb/s and 1.5 Gb/s only)	6 6 0

Notes:
1. PCI Legacy Mode may optionally be used allowing external PCI bus support through a PCIe-to-PCI bridge.

1.4 Device and Revision ID Table

The Revision ID (RID) register is an 8-bit register located at offset 08h in the PCI header of every PCI/PCIe function. The RID register is used by software to identify a particular component stepping when a driver change or patch unique to that stepping is needed.

Table 1-3. Intel® Xeon® Processor D-1500 Product Family Device and Revision ID (Sheet 1 of 2)

Device Function	Description	Dev ID	V1 SRID	Comments
D31:F2	SATA[1]	2822h	05h	If AIE (D31:F2 Offset 9Ch bit 7) = 0 AND AIES (D31:F2 Offset 9Ch bit 6) = 0.
		8C06h	05h	If AIE (D31:F2 Offset 9Ch bit 7) = 1.
		2826h	05h	If AIE (D31:F2 Offset 9Ch bit 7) = 0 AND AIES (D31:F2 Offset 9Ch bit 6) = 1.
		8C06h	05h	If AIE (D31:F2 Offset 9Ch bit 7) = 1.

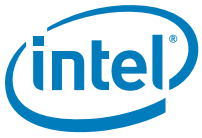


Table 1-3. Intel® Xeon® Processor D-1500 Product Family Device and Revision ID (Sheet 2 of 2)

Device Function	Description	Dev ID	V1 SRID	Comments
D31:F5	SATA	8C08h	05h	Non-AHCI and Non-RAID Mode (Ports 4 and 5)
D28:F0	PCI Express* Port 1	8C10h	05h	When D28:F0:ECh:bit 1= 0)
		244Eh	05h	When D28:F0:ECh:bit 1 = 1
D28:F1	PCI Express Port 2	8C12h	05h	When D28:F1:ECh:bit 1 = 0
		244Eh	05h	When D28:F1:ECh:bit 1 = 1
D28:F2	PCI Express Port 3	8C14h	05h	When D28:F2:ECh:bit 1 = 0
		244Eh	05h	When D28:F2:ECh:bit 1 = 1
D28:F3	PCI Express Port 4	8C16h	05h	When D28:F3:ECh:bit 1 = 0
		244Eh	05h	When D28:F3:ECh:bit 1 = 1
D28:F4	PCI Express Port 5	8C18h	05h	When D28:F4:ECh:bit 1 = 0
		244Eh	05h	When D28:F4:ECh:bit 1 = 1
D28:F5	PCI Express Port 6	8C1Ah	05h	When D28:F5:ECh:bit 1 = 0
		244Eh	05h	When D28:F5:ECh:bit 1 = 1
D28:F6	PCI Express Port 7	8C1Ch	05h	When D28:F6:ECh:bit 1 = 0
		244Eh	05h	When D28:F6:ECh:bit 1 = 1
D28:F7	PCI Express Port 8	8C1Eh	05h	When D28:F7:ECh:bit 1 = 0
		244Eh	05h	When D28:F7:ECh:bit 1 = 1
D31:F3	SMBus	8C22h	05h	All SKUs.
D31:F6	Thermal	8C24h	05h	All SKUs.
D29:F0	USB EHCI #1	8C26h	05h	All SKUs.
D20:F0	USB xHCI	8C31h	05h	All SKUs.
D25:F0	LAN	8C33h	05h	All SKUs.
D22:F0	Intel® ME Interface #1	8C3Ah	04h	All SKUs.
D22:F1	Intel ME Interface #2	8C3Bh	04h	All SKUs.
D22:F2	IDE-R	8C3Ch	04h	All SKUs.
D22:F3	KT	8C3Dh	04h	All SKUs.
D31:F0	LPC	8C54h	05h	LPC Controller

Notes:

1. PCH contains two SATA controllers. The SATA Device ID is dependent upon which SATA mode is selected by BIOS and what RAID capabilities exist in the SKU.
2. The SATA RAID Controller Device ID is dependent upon the AIE bit setting (bit 7 of D31:F2:Offset 9Ch).
3. SATA Controller 2 (D31:F5) is only visible when D31:F2 CC.SCC =01h.
4. LAN Device ID is loaded from EEPROM. If EEPROM contains either 0000h or FFFFh in the Device ID location, then 8C33h is used. Refer to the appropriate Intel® GbE physical layer Transceiver (PHY) datasheet for LAN Device IDs.
5. For a given stepping, not all SKUs may be available.

6. This table shows the default PCI Express Function Number-to-Root Port mapping. Function numbers for a given root port are assignable through the “Root Port Function Number and Hide for PCI Express Root Ports” register (RCBA+0404h).

§

2 Intel® Xeon® Processor D-1500 Product Family and System Clocks

Intel® Xeon® Processor D-1500 Product Family provides a complete system clocking solution through Integrated Clocking.

Intel® Xeon® Processor D-1500 Product Family-based platforms require several single-ended and differential clocks to synchronize signal operation and data propagation between system-wide interfaces, and across clock domains. In Integrated Clock mode, all the system clocks will be provided by Intel® Xeon® Processor D-1500 Product Family from a 25 MHz crystal-generated clock input.

The output signals from Intel® Xeon® Processor D-1500 Product Family are:

- One 100 MHz differential source for BCLK (PCI Express* 3.0 jitter tolerant)
- Eight 100 MHz differential sources for PCI Express 2.0 devices
- Two 100 MHz differential source for PCI Express Graphics devices (PCI Express 3.0 jitter tolerant)
- One 100 MHz differential clock for XDP/Intel ITP which can be used as a clock to a third PEG slot (PCI Express 3.0 jitter tolerant)
- Five 33 MHz single-ended source for other devices (One of these is reserved as loopback clock)
- Four flexible single-ended outputs that can be used for 14.31818/24/33/48 MHz for legacy platform functions, discrete graphics devices, external USB controllers, and so on.

2.1 Straps Related to Clock Configuration

Hardware functional straps (that is, pins): None required for clock configuration.

Soft straps implemented in the SPI flash device for Intel® Xeon® Processor D-1500 Product Family clock configuration: Integrated Clocking Profile Select (3 Profile select bits allow up to 8 different clock profiles to be specified). In addition, 3 RTC well backed host register bits are also defined for Integrated Clocking Profile Selection through BIOS.

2.2 SoC Clocking Requirements

Providing a platform-level clocking solution uses multiple system components including:

- The SoC
- 25 MHz crystal source

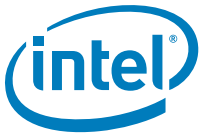
A summary is given in the following tables; Table 2-1 shows the system clock input to Intel® Xeon® Processor D-1500 Product Family. Table 2-2 shows system clock outputs generated by Intel® Xeon® Processor D-1500 Product Family.

Table 2-1. SoC Clock Inputs

Clock Domain	Frequency	Usage description
CLKIN_GND2_P/N	N/A	Unused. Tie each signal to GND through a 10 KΩ resistor.
CLKIN_GND3_P/N	N/A	Unused. Tie each signal to GND through a 10 KΩ resistor.
CLKIN_GND4_P/N	N/A	Unused. Tie each signal to GND through a 10 KΩ resistor.
CLKIN_GND_P/N	N/A	Unused. Tie each signal to GND through a 10 KΩ resistor.
CLKIN_33MHZLOOPBACK	33 MHz	33 MHz clock feedback input to reduce skew between Intel® Xeon® Processor D-1500 Product Family 33 MHz clocks and buses such as LPC. This signal must be connected to one of the pins in the group **CLKOUT_33MHz[4:0]**
REFCLK14IN	14.31818 MHz	Unused. Tie signal to GND through a 10 KΩ resistor.
XTAL25_IN	25 MHz	Crystal input source used by Intel® Xeon® Processor D-1500 Product Family.

Table 2-2. Clock Outputs

Clock Domain	Frequency	Spread Spectrum	Usage
CLKOUT_33MHz[4:0]	33 MHz	Yes	Single Ended 33 MHz outputs. One of these signals must be connected to **CLKIN_33MHZLOOPBACK** to function as a clock loopback. This allows skew control for variable lengths of **CLKOUT_33MHz[4:0]**.
CLKOUT_PCIE[7:0]_P/N	100 MHz	Yes	100 MHz PCIe 2.0 specification compliant differential output to PCI Express devices.
CLKOUT_PEG_A_P/N CLKOUT_PEG_B_P/N	100 MHz	Yes	100 MHz PCIe 3.0 specification compliant differential outputs to PCI Express Graphics devices.
CLKOUT_ITPXDP_P/N	100 MHz	Yes	Primarily used as 100 MHz Clock to processor XDP/Intel ITP on the platform or can be configured as CLKOUT_PEG_C_P/N.
CLKOUTFLEX1/ GPIO65 CLKOUTFLEX3/ GPIO67	33 MHz / 14.31818 MHz / 48 MHz / 24 MHz	Yes	Programmable 33 MHz, 48/24 MHz or 14.31818 MHz outputs for various platform devices.
SPI_CLK	17.86 MHz / 31.25 MHz / 50 MHz	No	Drive SPI devices connected to Intel® Xeon® Processor D-1500 Product Family. Generated by Intel® Xeon® Processor D-1500 Product Family.
XTAL25_OUT	25 MHz	No	Crystal output source by Intel® Xeon® Processor D-1500 Product Family.



2.3 Functional Blocks

Intel® Xeon® Processor D-1500 Product Family has 1 main PLL in which its output is divided down through Modulators and Dividers to provide great flexibility in clock source selection, configuration, and better power management. Table 2-3 describes the PLLs on Intel® Xeon® Processor D-1500 Product Family and the clock domains that are driven from the PLLs.

Table 2-3. Intel® Xeon® Processor D-1500 Product Family PLLs

PLL	Outputs[1]	Description/Usage
XCK_PLL	Four 2.7 GHz outputs 90° apart. Outputs are routed to each of the Spread Modulator blocks before hitting the various dividers and the other PLLs to provide clocks to all of the I/O interface logic. This PLL also provides 5.4 GHz and 2.7 GHz CMOS outputs for use by various dividers to create non-spread output clocks.	Main Reference PLL. Always enabled in Integrated Clocking mode. Resides in core power well and is not powered in S3 and below states. Powered in sub-S0 states by a Suspend well Ring oscillator.

Notes:
1. Indicates the source clock frequencies driven to other internal logic for delivering functionality needed. Does not indicate external outputs.

Spread Spectrum adjustment can be made without platform reboot. Table 2-4 provides a basic description of spread modulators that operate on the XCK PLL's 2.7 GHz outputs.

Table 2-4. Modulator Blocks

Modulator	Description
MOD1	Used for spread modulation, or bending, on 135 MHz clock to integrated graphics display. Typical display usage model is 0.5% down-spread. In certain usage case, this modulator can be shut off for 0% spread with or without clock bending. Used by the display driver only.
MOD2	Used for spread modulation and fine grain frequency synthesis on nominal 100 MHz overclockable clock to PEG. This modulator also subject to adaptive clocking adjustment (for EMC) when left on at nominal 100 MHz frequency.
MOD3	Used for spread modulation (and adaptive clocking) on 100 M Hz clock to processor PEG, PCIe*, USB 3.0, SATA, Single Ended 33 MHz, and Thermal Sensor.
MOD4	Used for fine grain frequency synthesis on nominal 135 MHz, non-spread clock to integrated graphics display. Used by the display driver only.
MOD5	Used for fine grain frequency synthesis of a wide variety of integrated graphics display VGA clocking needs. Used by the display driver only.
MOD6	Used for fine grain frequency synthesis of 96 MHz non-spread clock to USB PLL and Intel® Xeon® Processor D-1500 Product Family logic. 48/24 MHz to Flex Clocks are further derived from 96 MHz output.
MOD7	Used for fine grain frequency synthesis of 14.31818 MHz non-spread clock to Flex Clocks and Intel® Xeon® Processor D-1500 Product Family logic.

2.4 Clock Configuration Access Overview

Intel® Xeon® Processor D-1500 Product Family provides increased flexibility of host equivalent configurability of clocks, using Intel® ME FW.

In the Intel® Management Engine FW assisted configuration mode, control settings for PLLs, Spread Modulators, and other clock configuration registers will be handled by the Intel® Management Engine. The parameters to be loaded will reside in the Intel® Management Engine data region of the SPI Flash device.
BIOS would only have access to the register set through a set of MEI commands to the Intel® Management Engine.

2.5 Integrated Clock Controller (ICC) Registers

This section describes all registers and base functionality that is related to the Integrated Clock Controller. The ICC registers are not visible using PCI Configuration access and it is not mapped to I/O memory as other devices within Intel® Xeon® Processor D-1500 Product Family. The control settings for the ICC clock structure is located in registers directly under the control of the Intel® Management Engine.

ICC register access is only accessible using Intel® Management Engine FW and must be programmed using available FW access tools. The ICC registers disclosed in this chapter cover user adjustable features within the ICC subsystem programmable through available FW access tools.

2.5.1 ICC Registers under Intel® Management Engine (Intel® ME) Control

Table 2-5. ICC Registers under Intel® Management Engine (Intel® ME) Control

Mnemonic	Register Name	Default
SSCDIVINPHASE_PCHPCIE100	100 MHz SSC Divider Integer Phase Control for Intel® Xeon® Processor D-1500 Product Family PCIe Clocks	0000_0032h
SSCTRIPARAM_PCHPCIE100	100 MHz SSC Triangle Parameter for Intel® Xeon® Processor D-1500 Product Family PCIe Clocks	1240_4038h
SSCCTL_PCHPCIE100	100 MHz SSC Control for Intel® Xeon® Processor D-1500 Product Family PCIe Clocks	0000_0000h
DIV_PCI33	33 MHz Single Ended Clock Divide and Spread Enable	0003_0203h
DIV_FLEX4824	48/24 MHz Single Ended Flex Clock Divide Enable	0003_0103h
OCKEN	Output Clock Enables	7DFF_0F8Fh
SEFLXBP	Single Ended Flex Buffer Parameters	0000_9999h
SEPCICLKBP	Single Ended 33 MHz Clock Buffer Parameters	0009_9999h
DCOSS	Differential Clock Out Source Select	0000_0400h
SECOSS	Single Ended Clock Out Source Select	0000_2516h
MCSS	Miscellaneous Clock Source Select	0000_0001h
PLLRCS	PLL Reference Clock Select	0001_1114h
ICCCTL	ICC Control	0000_0008h
PMPCI	Power Management 33 MHz Clock	0000_0000h
PM1PCIECLK	Power Management 1 PCIe Clock	7654_3210h
PM2PCIECLK	Power Management 2 PCIe Clock	0000_0098h

2.5.1.1 SSCDIVINTPHASE_PCHPCIE100—100 MHz Intel® Xeon® Processor D-1500 Product Family PCIe Clock SSC Divider Integer Phase Register

Default Value: 00000032h
Attribute: R/W
Size: 32-bit

Bit	Description
31:0	**100 MHz PCIe* Clock SSC Phase Control** — R/W. This register is used for tuning PCIe Adaptive Clocking frequency. Firmware may program this field with various values when adjusting PCIe adaptive clocking values.

2.5.1.2 SSCTRIPARAM_PCHPCIE100—100 MHz Intel® Xeon® Processor D-1500 Product Family PCIe Clock SSC Triangle Register

Default Value: 12404038h
Attribute: R/W
Size: 32-bit

Bit	Description
31:0	**100 MHz PCIe Clock SSC Triangle Control** — R/W. This register is used for Intel® Xeon® Processor D-1500 Product Family PCIe clock SSC control. Firmware may program this field with various values when SSC is enabled.

2.5.1.3 SSCCTL_PCHPCIE100—100 MHz Intel® Xeon® Processor D-1500 Product Family PCIe* Clock SSC Control Register

Default Value: 00000000h
Attribute: R/W
Size: 32-bit

Bit	Description
31:0	**100 MHz PCIe Clock SSC Control** — R/W. This register is used for Intel® Xeon® Processor D-1500 Product Family PCIe clock SSC control. Should only use the default value.

2.5.1.4 DIV_PCI33—33 MHz Single Ended Clock Divide and Spread Enable Register

Default Value: 00030203h
Attribute: R/W
Size: 32-bit

Bit	Description
31:23	**Reserved**
22:21	**DIV_PCI33 Clock Mux Control 1**— R/W. Internal multiplex control for 33.33 MHz clock direction. 00 = 33.33 MHz SSC (Default) 10 = 33.33 MHz non-SSC All other values are not supported.
20:17	Reserved
16	**DIV_PCI33 Clock Mux Control 2** — R/W. Internal multiplex control for 33.33 MHz clock direction. 0 = 33.33 MHz SSC (Default) 1 = 33.33 MHz non-SSC
15	**DIV_PCI33 Enable/Disable** — R/W. 0 = Enables divider for SSC. (Default) 1 = Enables divider with no SSC.
14:13	Reserved
12	**DIV_PCI33 Clock Internal Gating Enable** — R/W. 0 = 33.33 MHz SSC (Default) 1 = 33.33 MHz non-SSC
11	Reserved
10:8	**DIV_PCI33 Divider Selection** — R/W. 010 =Divide by 3 from an internal 100 MHz clock source for 33 MHz single ended clocks. All other values are not supported.
7	Reserved
6:0	**DIV_PCI33 Divider Value Counter** — R/W. Bit value only valid when use in non-SSC configurations. 001_1001 = 33.33 MHz frequency All other values are not supported.

2.5.1.5 DIV_FLEX4824—48 MHz and 24 MHz Single Ended FLEX Clock Divide Enable Register

Default Value: 00030103h
Attribute: R/W
Size: 32-bit

Bit	Description
31:16	**Reserved**
15	**DIV_FLEX4824 Enable/Disable** — R/W. This register controls the 48 MHz and 24 MHz single ended FLEX clock divider from a 96 MHz internal clock source. 0 = Enables divider 1 = Disables divider
14:11	Reserved
10:8	**DIV_FLEX4824 Divider Selection** — R/W. 001 = Enables a divide by 2 from an internal 96 MHz clock source for 48 MHz single ended clock FLEX clock output frequency. (Default) 100 = Enables a divide by 4 from an internal 96 MHz clock source for a 24 MHz single ended clock FLEX clock output frequency. All other values are not supported.
7:0	Reserved

2.5.1.6 OCKEN—Output Clock Enable Register

Default Value: 7DFF0F8Fh
Attribute: R/W
Size: 32-bit

Bit	Description
31	Reserved
30	**DPNS Clock Output Clock Enable —** R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default) ***Note:*** This clock must be connected to the processor (and functional) regardless of internal graphics configuration support.
29	**DP Clock Output Clock Enable —** R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default)
28	Reserved
27	**PEG_B Clock Output Clock Enable —** R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default)
26	PEG_A Clock Output Clock Enable — R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default)
25	Reserved
24	ITPXDP Clock Output Clock Enable — R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default)
23	**PCIe* Clock 7 Output Clock Enable —** R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).
22	**PCIe Clock 6 Output Clock Enable —** R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).
21	**PCIe Clock 5 Output Clock Enable —** R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).

Bit	Description
20	**PCIe Clock 4 Output Clock Enable —** R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).
19	**PCIe Clock 3 Output Clock Enable —** R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).
18	**PCIe Clock 2 Output Clock Enable —** R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).
17	**PCIe Clock 1 Output Clock Enable —** R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).
16	**PCIe* Clock 0 Output Clock Enable —** R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).
15:12	Reserved
11	**33MHz Clock 4 Output Clock Enable —** R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).
10	33 MHz Clock 3 Output Clock Enable — R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).
9	33MHz Clock 2 Output Clock Enable — R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).
8	33MHz Clock 1 Output Clock Enable — R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).
7	33MHz Clock 0 Output Clock Enable — R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).
6:4	Reserved
3	FLEX Clock 3 Output Clock Enable — R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).
2	Reserved
1	FLEX Clock 1 Output Clock Enable — R/W. 0 = Output is gated to a low state. 1 = Output is enabled to toggle (Default).
0	Reserved

2.5.1.7 SEFLXBP—Single Ended Flex Buffer Parameter Register

Default Value: 00009999h

Attribute: R/W

Size: 32-bit

Bit	Description
31:16	Reserved
15:13	**FLEX3 Clock Buffer Slew Rate Selection —** R/W. This parameter controls slew rate of FLEX clock 3. Each bit step change corresponds to ~0.2 V/ns. 000 = 0.6 V/ns minimum 100 = 1.4 V/ns (Default) 111 = 2.0 V/ns maximum

Bit	Description
12	FLEX3 Clock Buffer Resistance Selection — R/W. This parameter controls Single/Double load series resistance. 0 = 25 Ω single load usage 1 = 17 Ω double load usage (Default).
11:8	Reserved
7:5	**FLEX1 Clock Buffer Slew Rate Selection —** R/W. This parameter controls slew rate of FLEX clock 3. Each bit step change corresponds to ~0.2 V/ns. 000 = 0.6 V/ns minimum 100 = 1.4 V/ns (Default) 111 = 2.0 V/ns maximum
4	FLEX1 Clock Buffer Resistance Selection — R/W. This parameter controls Single/Double load series resistance. 0 = 25Ω single load usage 1 = 17Ω double load usage (Default).
3:0	Reserved

2.5.1.8 SEPCICLKBP—Single Ended 33 MHz Clock Buffer Parameter Register

Default Value: 00099999h
Attribute: R/W
Size: 32-bit

Bit	Description
31:20	Reserved
19:17	**CLKOUT_33MHz_4 Clock Buffer Slew Rate Selection —** R/W. This parameter controls slew rate of 33 MHz clock 4. Each bit step change corresponds to ~0.2 V/ns. 000 = 0.6 V/ns minimum 100 = 1.4 V/ns (Default) 111 = 2.0 V/ns maximum
16	CLKOUT_33MHz_4 Clock Buffer Resistance Selection — R/W. This parameter controls Single/ Double load series resistance. 0 = 25 Ω single load usage 1 = 17 Ω double load usage (Default).
15:13	**CLKOUT_33MHz_3 Clock Buffer Slew Rate Selection —** R/W. This parameter controls slew rate of 33 MHz clock 3. Each bit step change corresponds to ~0.2 V/ns. 000 = 0.6 V/ns minimum 100 = 1.4 V/ns (Default) 111 = 2.0 V/ns maximum
12	CLKOUT_33MHz_3 Clock Buffer Resistance Selection — R/W. This parameter controls Single/ Double load series resistance. 0 = 25 Ω single load usage 1 = 17 Ω double load usage (Default).
11:9	**CLKOUT_33MHz_2 Clock Buffer Slew Rate Selection —** R/W. This parameter controls slew rate of 33 MHz clock 2. Each bit step change corresponds to ~0.2 V/ns. 000 = 0.6 V/ns minimum 100 = 1.4 V/ns (Default) 111 = 2.0 V/ns maximum
8	CLKOUT_33MHz_2 Clock Buffer Resistance Selection — R/W. This parameter controls Single/ Double load series resistance. 0 = 25 Ω single load usage 1 = 17 Ω double load usage (Default).
7:5	**CLKOUT_33MHz_1 Clock Buffer Slew Rate Selection —** R/W. This parameter controls slew rate of 33 MHz clock 1. Each bit step change corresponds to ~0.2 V/ns. 000 = 0.6 V/ns minimum 100 = 1.4 V/ns (Default) 111 = 2.0 V/ns maximum

Bit	Description
4	CLKOUT_33MHz_1 Clock Buffer Resistance Selection — R/W. This parameter controls Single/ Double load series resistance. 0 = 25 Ω single load usage 1 = 17 Ω double load usage (Default).
3:1	**CLKOUT_33MHz_0 Clock Buffer Slew Rate Selection —** R/W. This parameter controls slew rate of 33 MHz clock 0. Each bit step change corresponds to ~0.2 V/ns. 000 = 0.6 V/ns minimum 100 = 1.4 V/ns (Default) 111 = 2.0 V/ns maximum
0	CLKOUT_33MHz_0 Clock Buffer Resistance Selection — R/W. This parameter controls Single/ Double load series resistance. 0 = 25 Ω single load usage 1 = 17 Ω double load usage (Default)

2.5.1.9 DCOSS—Differential Clock Out Source Select Register

Default Value: 00000400h
Attribute: R/W
Size: 32-bit

Bit	Description
31:10	Reserved
9:8	Reserved
7:6	**CLKOUT_PEGB Source Select —** R/W. This parameter selects the source of clock to be driven out on CLKOUT_PEGB. When not over-clocking this output should be sourced by the PCIe clock source MODIV3. 00 = Non-Overclockable source MODIV3 (Default) 01 = Reserved 10 = Reserved 11 = Reserved
5:4	**CLKOUT_PEGA Source Select —** R/W. This parameter selects the source of clock to be driven out on CLKOUT_PEGA. When not over-clocking this output should be sourced by the PCIe clock source MODIV3. 00 = Non-Overclockable source MODIV3 (Default) 01 = Reserved 10 = Reserved 11 = Reserved
3:0	Reserved

2.5.1.10 SECOSS—Single Ended Clock Out Source Select Register

Default Value: 00002516h
Attribute: R/W
Size: 32-bit

Bit	Description
31:15	Reserved
14:12	**CLKOUTFLEX3 Source Select —** R/W. This field selects the source of clock to be driven out on CLKOUTFLEX3. 000 = 33.33 MHz Clock Source 001 = 14.31818 MHz Clock Source 010 = 48/24 MHz Clock Source (Default) All other values are not supported.
11:7	Reserved
6:4	**CLKOUTFLEX1 Source Select** — R/W. This field selects the source of clock to be driven out on CLKOUTFLEX1. 000 = 33.33 MHz Clock Source 001 = 14.31818 MHz Clock Source (Default) 010 = 48/24 MHz Clock Source All other values are not supported.

Bit	Description
3:0	Reserved

2.5.1.11 ICCCTL—ICC Control Register

Default Value: 00000008h
Attribute: R/W
Size: 32-bit

Bit	Description
31:5	Reserved
4	**Dynamic Power Management for 96MHz Clock Source MODIV6 —** R/W. This field enables power management for all clocks that use this source to be brought down to the lowest power state when hardware detects an idle condition. 0 = Power Management is Disabled (Default) 1 = Power Management is Enabled
3	Reserved
2	**Warm Reset Gating of CLKOUT_DPNS —** R/W. This field enabled whether CLKOUT_DPNS is gated during Warm Reset. 0 = CLKOUT_DPNS is not gated (Default) 1 = CLKOUT_DPNS is gated
1	**Warm Reset Gating of CLKOUT_PEGA/PEGB —** R/W. This field enabled whether CLKOUT_PEGA/PEGB are gated during Warm Reset. 0 = CLKOUT_PEGA/PEGB are not gated (Default) 1 = CLKOUT_PEGA/PEGB are gated
0	Reserved

2.5.1.12 PMPCI—33MHz Single Ended Clock Power Management Register

Default Value: 00000000h
Attribute: R/W
Size: 32-bit

Bit	Description
31:9	Reserved
8	**CLKRUN Control Enable for 33 MHz Single Ended Clocks on CLKOUTFLEX3 —** R/W. Controls the enabling of support for CLKRUN protocol for 33 MHz clocks multiplexed out on CLKOUTFLEX3 pin. 0 = CLKRUN Control is disabled and clock is free running (Default) 1 = CLKRUN Control is enabled and clock output can be turned off
7	Reserved
6	**CLKRUN Control Enable for 33 MHz Single Ended Clocks on CLKOUTFLEX1 —** R/W. Controls the enabling of support for CLKRUN protocol for 33 MHz clocks multiplexed out on CLKOUTFLEX1 pin. 0 = CLKRUN Control is disabled and clock is free running (Default) 1 = CLKRUN Control is enabled and clock output can be turned off
5	Reserved
4	**CLKRUN Control Enable for fixed 33 MHz Single Ended Clock Output 4 —** R/W**.** Controls the enabling of support for CLKRUN protocol for fixed 33 MHz clock outputs. 0 = CLKRUN Control is disabled and clock is free running (Default) 1 = CLKRUN Control is enabled and clock output can be turned off
3	**CLKRUN Control Enable for fixed 33 MHz Single Ended Clock Output 3 —** R/W**.** Controls the enabling of support for CLKRUN protocol for fixed 33 MHz clock outputs. 0 = CLKRUN Control is disabled and clock is free running (Default) 1 = CLKRUN Control is enabled and clock output can be turned off
2	**CLKRUN Control Enable for fixed 33 MHz Single Ended Clock Output 2 —** R/W**.** Controls the enabling of support for CLKRUN protocol for fixed 33 MHz clock outputs. 0 = CLKRUN Control is disabled and clock is free running (Default) 1 = CLKRUN Control is enabled and clock output can be turned off

Bit	Description
1	**CLKRUN Control Enable for fixed 33 MHz Single Ended Clock Output 1 —** R/W**.** Controls the enabling of support for CLKRUN protocol for fixed 33 MHz clock outputs. 0 = CLKRUN Control is disabled and clock is free running (Default) 1 = CLKRUN Control is enabled and clock output can be turned off
0	**CLKRUN Control Enable for fixed 33 MHz Single Ended Clock Output 0 —** R/W**.** Controls the enabling of support for CLKRUN protocol for fixed 33 MHz clock outputs. 0 = CLKRUN Control is disabled and clock is free running (Default) 1 = CLKRUN Control is enabled and clock output can be turned off

2.5.1.13 PM1PCIECLK—Power Management 1 PCIe Clock Register

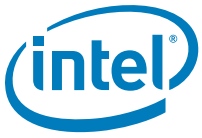
Default Value: 76543210h

Attribute: R/W

Size: 32-bit

Bit	Description
31:28	**CLKRQ# Select for CLKOUT_PCIE7_P/N —** R/W**.** Select version of external input CLKRQ# for dynamic control of the output CLKOUT_PCIE7_P/N. 0000 = PCIECLKRQ0# controls CLKOUT_PCIE7_P/N 0001 = PCIECLKRQ1# controls CLKOUT_PCIE7_P/N 0010 = PCIECLKRQ2# controls CLKOUT_PCIE7_P/N 0011 = PCIECLKRQ3# controls CLKOUT_PCIE7_P/N 0100 = PCIECLKRQ4# controls CLKOUT_PCIE7_P/N 0101 = PCIECLKRQ5# controls CLKOUT_PCIE7_P/N 0110 = PCIECLKRQ6# controls CLKOUT_PCIE7_P/N 0111 = PCIECLKRQ7# controls CLKOUT_PCIE7_P/N (Default) 1000 = PEG_A_CLKRQ# controls CLKOUT_PCIE7_P/N 1001 = PEG_B_CLKRQ# controls CLKOUT_PCIE7_P/N 1010 – 1111 = RSVD
27:24	**CLKRQ# Select for CLKOUT_PCIE6_P/N —** R/W**.** Select version of external input CLKRQ# for dynamic control of the output CLKOUT_PCIE6_P/N. 0000 = PCIECLKRQ0# controls CLKOUT_PCIE6_P/N 0001 = PCIECLKRQ1# controls CLKOUT_PCIE6_P/N 0010 = PCIECLKRQ2# controls CLKOUT_PCIE6_P/N 0011 = PCIECLKRQ3# controls CLKOUT_PCIE6_P/N 0100 = PCIECLKRQ4# controls CLKOUT_PCIE6_P/N 0101 = PCIECLKRQ5# controls CLKOUT_PCIE6_P/N 0110 = PCIECLKRQ6# controls CLKOUT_PCIE6_P/N (Default) 0111 = PCIECLKRQ7# controls CLKOUT_PCIE6_P/N 1000 = PEG_A_CLKRQ# controls CLKOUT_PCIE6_P/N 1001 = PEG_B_CLKRQ# controls CLKOUT_PCIE76_P/N 1010 – 1111 = RSVD
23:20	**CLKRQ# Select for CLKOUT_PCIE5_P/N —** R/W**.** Select version of external input CLKRQ# for dynamic control of the output CLKOUT_PCIE5_P/N. 0000 = PCIECLKRQ0# controls CLKOUT_PCIE5_P/N 0001 = PCIECLKRQ1# controls CLKOUT_PCIE5_P/N 0010 = PCIECLKRQ2# controls CLKOUT_PCIE5_P/N 0011 = PCIECLKRQ3# controls CLKOUT_PCIE5_P/N 0100 = PCIECLKRQ4# controls CLKOUT_PCIE5_P/N 0101 = PCIECLKRQ5# controls CLKOUT_PCIE5_P/N (Default) 0110 = PCIECLKRQ6# controls CLKOUT_PCIE5_P/N 0111 = PCIECLKRQ7# controls CLKOUT_PCIE5_P/N 1000 = PEG_A_CLKRQ# controls CLKOUT_PCIE5_P/N 1001 = PEG_B_CLKRQ# controls CLKOUT_PCIE5_P/N 1010 – 1111 = RSVD

Bit	Description
19:16	**CLKRQ# Select for CLKOUT_PCIE4_P/N —** R/W**.** Select version of external input CLKRQ# for dynamic control of the output CLKOUT_PCIE4_P/N. 0000 = PCIECLKRQ0# controls CLKOUT_PCIE4_P/N 0001 = PCIECLKRQ1# controls CLKOUT_PCIE4_P/N 0010 = PCIECLKRQ2# controls CLKOUT_PCIE4_P/N 0011 = PCIECLKRQ3# controls CLKOUT_PCIE4_P/N 0100 = PCIECLKRQ4# controls CLKOUT_PCIE4_P/N (Default) 0101 = PCIECLKRQ5# controls CLKOUT_PCIE4_P/N 0110 = PCIECLKRQ6# controls CLKOUT_PCIE4_P/N 0111 = PCIECLKRQ7# controls CLKOUT_PCIE4_P/N 1000 = PEG_A_CLKRQ# controls CLKOUT_PCIE4_P/N 1001 = PEG_B_CLKRQ# controls CLKOUT_PCIE4_P/N 1010 – 1111 = RSVD
15:12	**CLKRQ# Select for CLKOUT_PCIE3_P/N —** R/W**.** Select version of external input CLKRQ# for dynamic control of the output CLKOUT_PCIE3_P/N. 0000 = PCIECLKRQ0# controls CLKOUT_PCIE3_P/N 0001 = PCIECLKRQ1# controls CLKOUT_PCIE3_P/N 0010 = PCIECLKRQ2# controls CLKOUT_PCIE3_P/N 0011 = PCIECLKRQ3# controls CLKOUT_PCIE3_P/N (Default) 0100 = PCIECLKRQ4# controls CLKOUT_PCIE3_P/N 0101 = PCIECLKRQ5# controls CLKOUT_PCIE3_P/N 0110 = PCIECLKRQ6# controls CLKOUT_PCIE3_P/N 0111 = PCIECLKRQ7# controls CLKOUT_PCIE3_P/N 1000 = PEG_A_CLKRQ# controls CLKOUT_PCIE3_P/N 1001 = PEG_B_CLKRQ# controls CLKOUT_PCIE3_P/N 1010 – 1111 = RSVD
11:8	**CLKRQ# Select for CLKOUT_PCIE2_P/N —** R/W**.** Select version of external input CLKRQ# for dynamic control of the output CLKOUT_PCIE2_P/N. 0000 = PCIECLKRQ0# controls CLKOUT_PCIE2_P/N 0001 = PCIECLKRQ1# controls CLKOUT_PCIE2_P/N 0010 = PCIECLKRQ2# controls CLKOUT_PCIE2_P/N (Default) 0011 = PCIECLKRQ3# controls CLKOUT_PCIE2_P/N 0100 = PCIECLKRQ4# controls CLKOUT_PCIE2_P/N 0101 = PCIECLKRQ5# controls CLKOUT_PCIE2_P/N 0110 = PCIECLKRQ6# controls CLKOUT_PCIE2_P/N 0111 = PCIECLKRQ7# controls CLKOUT_PCIE2_P/N 1000 = PEG_A_CLKRQ# controls CLKOUT_PCIE2_P/N 1001 = PEG_B_CLKRQ# controls CLKOUT_PCIE2_P/N 1010 – 1111 = RSVD
7:4	**CLKRQ# Select for CLKOUT_PCIE1_P/N —** R/W**.** Select version of external input CLKRQ# for dynamic control of the output CLKOUT_PCIE1_P/N. 0000 = PCIECLKRQ0# controls CLKOUT_PCIE1_P/N 0001 = PCIECLKRQ1# controls CLKOUT_PCIE1_P/N (Default) 0010 = PCIECLKRQ2# controls CLKOUT_PCIE1_P/N 0011 = PCIECLKRQ3# controls CLKOUT_PCIE1_P/N 0100 = PCIECLKRQ4# controls CLKOUT_PCIE1_P/N 0101 = PCIECLKRQ5# controls CLKOUT_PCIE1_P/N 0110 = PCIECLKRQ6# controls CLKOUT_PCIE1_P/N 0111 = PCIECLKRQ7# controls CLKOUT_PCIE1_P/N 1000 = PEG_A_CLKRQ# controls CLKOUT_PCIE1_P/N 1001 = PEG_B_CLKRQ# controls CLKOUT_PCIE1_P/N 1010 – 1111 = RSVD



Bit	Description
3:0	**CLKRQ# Select for CLKOUT_PCIE0_P/N —** R/W**.** Select version of external input CLKRQ# for dynamic control of the output CLKOUT_PCIE0_P/N. 0000 = PCIECLKRQ0# controls CLKOUT_PCIE0_P/N (Default) 0001 = PCIECLKRQ1# controls CLKOUT_PCIE0_P/N 0010 = PCIECLKRQ2# controls CLKOUT_PCIE0_P/N 0011 = PCIECLKRQ3# controls CLKOUT_PCIE0_P/N 0100 = PCIECLKRQ4# controls CLKOUT_PCIE0_P/N 0101 = PCIECLKRQ5# controls CLKOUT_PCIE0_P/N 0110 = PCIECLKRQ6# controls CLKOUT_PCIE0_P/N 0111 = PCIECLKRQ7# controls CLKOUT_PCIE0_P/N 1000 = PEG_A_CLKRQ# controls CLKOUT_PCIE0_P/N 1001 = PEG_B_CLKRQ# controls CLKOUT_PCIE0_P/N 1010 – 1111 = RSVD

2.5.1.14 PM2PCIECLK—Power Management 2 PCIe Clock Register

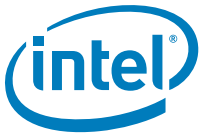
Attribute: R/W

Default Value: 00000098h Size: 32-bit

Bit	Description
31:27	Reserved
26	**Enable CLKREQ# for CLKOUT_ ITPXDP_P/N —** R/W**.** Enable dynamic control of CLKOUT_ ITPXDP_P/N by the mapped CLKREQ#. This register bit may be updated dynamically. 0 = Disable dynamic control of CLKOUT_ ITPXDP_P/N (Default) 1 = Enable dynamic control of CLKOUT_ ITPXDP_P/N
25	**Enable CLKREQ# for CLKOUT_ PEG_B_P/N —** R/W**.** Enable dynamic control of CLKOUT_PEG_B_P/N by the mapped CLKREQ#. This register bit may be updated dynamically. 0 = Disable dynamic control of CLKOUT_PEG_B_P/N (Default) 1 = Enable dynamic control of CLKOUT_PEG_B_P/N
24	**Enable CLKREQ# for CLKOUT_ PEG_A_P/N —** R/W**.** Enable dynamic control of CLKOUT_ PEG_A_P/N by the mapped CLKREQ#. This register bit may be updated dynamically. 0 = Disable dynamic control of CLKOUT_ PEG_A_P/N (Default) 1 = Enable dynamic control of CLKOUT_ PEG_A_P/N
23	**Enable CLKREQ# for CLKOUT_ PCIE7_P/N —** R/W**.** Enable dynamic control of CLKOUT_ PCIE7_P/N by the mapped CLKREQ#. This register bit may be updated dynamically. 0 = Disable dynamic control of CLKOUT_ PCIE7_P/N (Default) 1 = Enable dynamic control of CLKOUT_ PCIE7_P/N
22	**Enable CLKREQ# for CLKOUT_ PCIE6_P/N —** R/W**.** Enable dynamic control of CLKOUT_ PCIE6_P/N by the mapped CLKREQ#. This register bit may be updated dynamically. 0 = Disable dynamic control of CLKOUT_ PCIE6_P/N (Default) 1 = Enable dynamic control of CLKOUT_ PCIE6_P/N
21	**Enable CLKREQ# for CLKOUT_ PCIE5_P/N —** R/W**.** Enable dynamic control of CLKOUT_ PCIE5_P/N by the mapped CLKREQ#. This register bit may be updated dynamically. 0 = Disable dynamic control of CLKOUT_ PCIE5_P/N (Default) 1 = Enable dynamic control of CLKOUT_ PCIE5_P/N
20	**Enable CLKREQ# for CLKOUT_ PCIE4_P/N —** R/W**.** Enable dynamic control of CLKOUT_ PCIE4_P/N by the mapped CLKREQ#. This register bit may be updated dynamically. 0 = Disable dynamic control of CLKOUT_ PCIE4_P/N (Default) 1 = Enable dynamic control of CLKOUT_ PCIE4_P/N
19	**Enable CLKREQ# for CLKOUT_ PCIE3_P/N —** R/W**.** Enable dynamic control of CLKOUT_ PCIE3_P/N by the mapped CLKREQ#. This register bit may be updated dynamically. 0 = Disable dynamic control of CLKOUT_ PCIE3_P/N (Default) 1 = Enable dynamic control of CLKOUT_ PCIE3_P/N
18	**Enable CLKREQ# for CLKOUT_ PCIE2_P/N —** R/W**.** Enable dynamic control of CLKOUT_ PCIE2_P/N by the mapped CLKREQ#. This register bit may be updated dynamically. 0 = Disable dynamic control of CLKOUT_ PCIE2_P/N (Default) 1 = Enable dynamic control of CLKOUT_ PCIE2_P/N

Bit	Description
17	**Enable CLKREQ# for CLKOUT_ PCIE1_P/N —** R/W. Enable dynamic control of CLKOUT_ PCIE1_P/N by the mapped CLKREQ#. This register bit may be updated dynamically. 0 = Disable dynamic control of CLKOUT_ PCIE1_P/N (Default) 1 = Enable dynamic control of CLKOUT_ PCIE1_P/N
16	**Enable CLKREQ# for CLKOUT_ PCIE0_P/N —** R/W**.** Enable dynamic control of CLKOUT_ PCIE0_P/N by the mapped CLKREQ#. This register bit may be updated dynamically. 0 = Disable dynamic control of CLKOUT_ PCIE0_P/N (Default) 1 = Enable dynamic control of CLKOUT_ PCIE0_P/N
15:12	Reserved
11:8	**CLKRQ# Select for CLKOUT_ITPXDP_P/N —** R/W**.** Select version of external input CLKRQ# for dynamic control of the output CLKOUT_ITPXDP_P/N. 0000 = PCIECLKRQ0# (GPIO 73) controls CLKOUT_ITPXDP_P/N (Default) 0001 = PCIECLKRQ1# (GPIO 18) controls CLKOUT_ITPXDP_P/N 0010 = PCIECLKRQ2# (GPIO 20) controls CLKOUT_ITPXDP_P/N 0011 = PCIECLKRQ3# (GPIO 25) controls CLKOUT_ITPXDP_P/N 0100 = PCIECLKRQ4# (GPIO 26) controls CLKOUT_ITPXDP_P/N 0101 = PCIECLKRQ5# (GPIO 44) controls CLKOUT_ITPXDP_P/N 0110 = PCIECLKRQ6# (GPIO 45) controls CLKOUT_ITPXDP_P/N 0111 = PCIECLKRQ7# (GPIO 46) controls CLKOUT_ITPXDP_P/N 1000 = PEG_A_CLKRQ# controls CLKOUT_ITPXDP_P/N 1001 = PEG_B_CLKRQ# controls CLKOUT_ITPXDP_P/N 1010 – 1111 = RSVD
7:4	**CLKRQ# Select for CLKOUT_PEG_B_P/N —** R/W**.** Select version of external input CLKRQ# for dynamic control of the output CLKOUT_PEG_B_P/N. 0000 = PCIECLKRQ0# (GPIO 73) controls CLKOUT_PEG_B_P/N 0001 = PCIECLKRQ1# (GPIO 18) controls CLKOUT_PEG_B_P/N 0010 = PCIECLKRQ2# (GPIO 20) controls CLKOUT_PEG_B_P/N 0011 = PCIECLKRQ3# (GPIO 25) controls CLKOUT_PEG_B_P/N 0100 = PCIECLKRQ4# (GPIO 26) controls CLKOUT_PEG_B_P/N 0101 = PCIECLKRQ5# (GPIO 44) controls CLKOUT_PEG_B_P/N 0110 = PCIECLKRQ6# (GPIO 45) controls CLKOUT_PEG_B_P/N 0111 = PCIECLKRQ7# (GPIO 46) controls CLKOUT_PEG_B_P/N 1000 = PEG_A_CLKRQ# controls CLKOUT_PEG_B_P/N 1001 = PEG_B_CLKRQ# controls CLKOUT_PEG_B_P/N (Default) 1010 – 1111 = RSVD
3:0	**CLKRQ# Select for CLKOUT_PEG_A_P/N —** R/W**.** Select version of external input CLKRQ# for dynamic control of the output CLKOUT_PEG_A_P/N. 0000 = PCIECLKRQ0# (GPIO 73) controls CLKOUT_PEG_A_P/N 0001 = PCIECLKRQ1# (GPIO 18) controls CLKOUT_PEG_A_P/N 0010 = PCIECLKRQ2# (GPIO 20) controls CLKOUT_PEG_A_P/N 0011 = PCIECLKRQ3# (GPIO 25) controls CLKOUT_PEG_A_P/N 0100 = PCIECLKRQ4# (GPIO 26) controls CLKOUT_PEG_A_P/N 0101 = PCIECLKRQ5# (GPIO 44) controls CLKOUT_PEG_A_P/N 0110 = PCIECLKRQ6# (GPIO 45) controls CLKOUT_PEG_A_P/N 0111 = PCIECLKRQ7# (GPIO 46) controls CLKOUT_PEG_A_P/N 1000 = PEG_A_CLKRQ# controls CLKOUT_PEG_A_P/N (Default) 1001 = PEG_B_CLKRQ# controls CLKOUT_PEG_A_P/N 1010 – 1111 = RSVD

§



3 Functional Description

This chapter describes the functions and interfaces of Intel® Xeon® Processor D-1500 Product Family.

3.1 PCI-to-PCI Bridge

The PCI-to-PCI bridge resides in PCI. The arbitration for the PCI bus is handled by this PCI device. The PCI decoder in this device must decode the ranges for the SoC. All register contents are lost when core well power is removed.

To provide for true isochronous transfers and configurable Quality of Service (QoS) transactions, Intel® Xeon® Processor D-1500 Product Family supports two virtual channels VC0 and VC1. These two channels provide a fixed arbitration scheme where VC1 is always the highest priority. VC0 is always enabled. VC1 must be specifically enabled and configured in the SoC.

3.1.1 PCI Legacy Mode

PCI functionality is not supported on new generation of Intel® Xeon® Processor D-1500 Product Family requiring methods such as using PCIe*-to-PCI bridges to enable external PCI I/O devices. To be able to use PCIe-to-PCI bridges and attached legacy PCI devices, Intel® Xeon® Processor D-1500 Product Family provides PCI Legacy Mode. PCI Legacy Mode allows both the PCI Express* root port and PCIe-to-PCI bridge look like subtractive PCI-to-PCI bridges. This allows the PCI Express root port to subtractively decode and forward legacy cycles to the bridge, and the PCIe-to-PCI bridge continues forwarding legacy cycles to downstream PCI devices.

Note: Software must ensure that only one Intel® Xeon® Processor D-1500 Product Family device is enabled for Subtractive decode at a time.

3.2 PCI Express* Root Ports (D28:F0~F7)

There are eight root ports available in Intel® Xeon® Processor D-1500 Product Family. The root ports are compliant to the PCI Express 2.0 specification running at 5.0 GT/s. The ports all reside in Device 28, and take Function 0 – 7. Port 1 is Function 0, Port 2 is Function 1, Port 3 is Function 2, Port 4 is Function 3, Port 5 is Function 4, Port 6 is Function 5, Port 7 is Function 6, and Port 8 is Function 7.

Note: This section assumes the default PCI Express Function Number-to-Root Port mapping is used. Function numbers for a given root port are assignable through the Root Port Function Number and Hide for PCI Express Root Ports register (RCBA+404h). In accordance with the PCI Local Bus Specification, all multi-function devices must have a Function 0 assigned.

3.2.1 Supported PCIe* Port Configurations

PCI Express Root Ports 1–4 or Ports 5–8 can independently be configured as four x1s, two x2s, one x2 and two x1s, or one x4 port widths, as shown in Table 3-1 and Table 3-2.

Function disable is covered in Section 5.1.63.

Table 3-1. PCI Express* Ports 1 Through 4 - Supported Configurations

Port 1	Port 2	Port 3	Port 4
x4			
x2		x2	
x2		x1	x1
x1	x1	x1	x1

Table 3-2. PCI Express Ports 5 Through 8 - Supported Configurations

Port 5	Port 6	Port 7	Port 8
x4			
x2		x2	
x2		x1	x1
x1	x1	x1	x1

3.2.2 Interrupt Generation

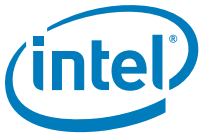
The root port generates interrupts on behalf of Hot-Plug and power management events, when enabled. These interrupts can either be pin based, or can be MSIs, when enabled.

When an interrupt is generated using the legacy pin, the pin is internally routed to Intel® Xeon® Processor D-1500 Product Family interrupt controllers. The pin that is driven is based upon the setting of the chipset configuration registers. Specifically, the chipset configuration registers used are the D28IP (Base address + 310Ch) and D28IR (Base address + 3146h) registers.

Table 3-3 summarizes interrupt behavior for MSI and wire-modes. In the table "bits" refers to the Hot-Plug and PME interrupt bits.

Table 3-3. MSI versus PCI IRQ Actions

Interrupt Register	Wire-Mode Action	MSI Action
All bits 0	Wire inactive	No action
One or more bits set to 1	Wire active	Send message
One or more bits set to 1, new bit gets set to 1	Wire active	Send message
One or more bits set to 1, software clears some (but not all) bits	Wire active	Send message
One or more bits set to 1, software clears all bits	Wire inactive	No action
Software clears one or more bits, and one or more bits are set on the same clock	Wire active	Send message



3.2.3 Power Management

3.2.3.1 S4/S5 Support

Software initiates the transition to S4/S5 by performing an I/O write to the Power Management Control register in Intel® Xeon® Processor D-1500 Product Family. After the I/O write completion has been returned to the processor, each root port will send a PME_Turn_Off TLP (Transaction Layer Packet) message on its downstream link. The device attached to the link will eventually respond with a PME_TO_Ack TLP message followed by sending a PM_Enter_L23 DLLP (Data Link Layer Packet) request to enter the L2/L3 Ready state. When all of Intel® Xeon® Processor D-1500 Product Family root ports links are in the L2/L3 Ready state, Intel® Xeon® Processor D-1500 Product Family power management control logic will proceed with the entry into S4/S5.

Prior to entering S4, software is required to put each device into $D3_{HOT}$. When a device is put into $D3_{HOT}$, it will initiate entry into a L1 link state by sending a PM_Enter_L1 DLLP. Thus, under normal operating conditions when the root ports sends the PME_Turn_Off message, the link will be in state L1. However, when the root port is instructed to send the PME_Turn_Off message, it will send it whether or not the link was in L1. Endpoints attached to Intel® Xeon® Processor D-1500 Product Family can make no assumptions about the state of the link prior to receiving a PME_Turn_Off message.

3.2.3.2 Resuming from Suspended State

The root port contains enough circuitry in the suspend well to detect a wake event through the WAKE# signal and to wake the system. When WAKE# is detected asserted, an internal signal is sent to the power management controller of Intel® Xeon® Processor D-1500 Product Family to cause the system to wake up. This internal message is not logged in any register, nor is an interrupt/GPE generated due to it.

3.2.3.3 Device Initiated PM_PME Message

When the system has returned to a working state from a previous low power state, a device requesting service will send a PM_PME message continuously, until acknowledged by the root port. The root port will take different actions depending upon whether this is the first PM_PME that has been received, or whether a previous message has been received but not yet serviced by the operating system.

If this is the first message received (RSTS.PS - D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 60h:bit 16 is cleared), the root port will set RSTS.PS, and log the PME Requester ID into RSTS.RID (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 60h:bits 15:0). If an interrupt is enabled using RCTL.PIE (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 5Ch:bit 3), an interrupt will be generated. This interrupt can be either a pin or an MSI if MSI is enabled using MC.MSIE (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 82h:Bit 0). See Section 3.2.3.4 for SMI/SCI generation.

If this is a subsequent message received (RSTS.PS is already set), the root port will set RSTS.PP (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 60h:Bit 17) and log the PME Requester ID from the message in a hidden register. No other action will be taken.

When the first PME event is cleared by software clearing RSTS.PS, the root port will set RSTS.PS, clear RSTS.PP, and move the requester ID from the hidden register into RSTS.RID.

If RCTL.PIE is set, an interrupt will be generated. If RCTL.PIE is not set, a message will be sent to the power management controller so that a GPE can be set. If messages have been logged (RSTS.PS is set), and RCTL.PIE is later written from a 0 to a 1, an interrupt will be generated. This last condition handles the case where the message was received prior to the operating system re-enabling interrupts after resuming from a low power state.

3.2.3.4 SMI/SCI Generation

Interrupts for power management events are not supported on legacy operating systems. To support power management on non-PCI Express aware operating systems, PM events can be routed to generate SCI. To generate SCI, MPC.PMCE must be set. When set, a power management event will cause SMSCS.PMCS (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset DCh:Bit 31) to be set.

Additionally, BIOS workarounds for power management can be supported by setting MPC.PMME (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset D8h:Bit 0). When this bit is set, power management events will set SMSCS.PMMS (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset DCh:Bit 0), and SMI # will be generated. This bit will be set regardless of whether interrupts or SCI is enabled. The SMI# may occur concurrently with an interrupt or SCI.

3.2.3.5 Latency Tolerance Reporting (LTR)

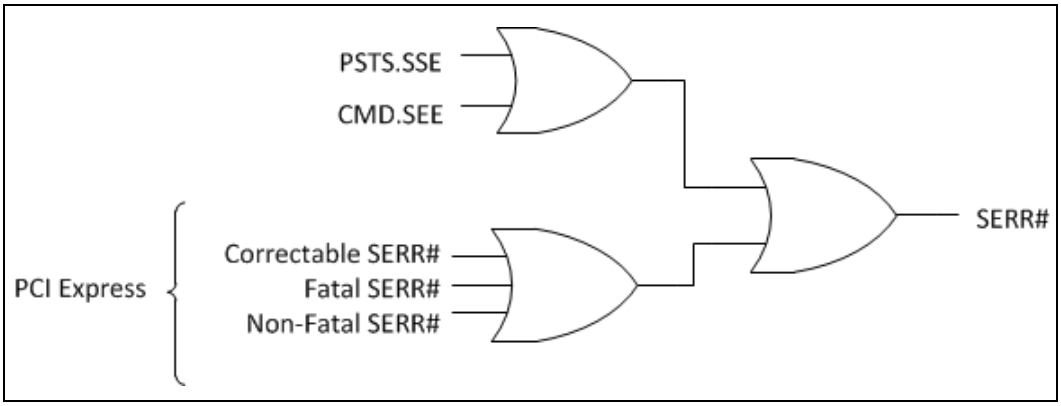
The root port supports the extended Latency Tolerance Reporting (LTR) capability. LTR provides a means for device endpoints to dynamically report their service latency requirements for memory access to the root port. Endpoint devices should transmit a new LTR message to the root port each time its latency tolerance changes (and initially during boot). Intel® Xeon® Processor D-1500 Product Family uses the information to make better power management decision. The processor uses the worst case tolerance value communicated by Intel® Xeon® Processor D-1500 Product Family to optimize c-state transitions. This results in better platform power management without impacting endpoint functionality.

Note: Endpoint devices the support LTR must implement the reporting and enable mechanism detailed in the PCIe* Latency Tolerance Reporting Engineering Change Notice.

3.2.4 SERR# Generation

SERR# may be generated using two paths – through PCI mechanisms involving bits in the PCI header, or through PCI Express* mechanisms involving bits in the PCI Express capability structure.

Figure 3-1. Generation of SERR# to Platform



3.2.5 Hot-Plug

Each root port implements a Hot-Plug controller that performs the following:

- Messages to turn on/off/blink LEDs
- Presence and attention button detection
- Interrupt generation

The root port only allows Hot-Plug with modules (such as ExpressCard*). Edge-connector based Hot-Plug is not supported.

3.2.5.1 Presence Detection

When a module is plugged in and power is supplied, the physical layer will detect the presence of the device, and the root port sets SLSTS.PDS (D28:F0/F1/F2/F3/F4/F5:Offset 5Ah:Bit 6) and SLSTS.PDC (D28:F0/F1/F2/F3:Offset 6h:Bit 3). If SLCTL.PDE (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 58h:Bit 3) and SLCTL.HPE (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 58h:Bit 5) are both set, the root port will also generate an interrupt.

When a module is removed (using the physical layer detection), the root port clears SLSTS.PDS and sets SLSTS.PDC. If SLCTL.PDE and SLCTL.HPE are both set, the root port will also generate an interrupt.

3.2.5.2 Message Generation

When system software writes to SLCTL.AIC (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 58h:Bits 7:6) or SLCTL.PIC (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 58h:Bits 9:8), the root port will send a message down the link to change the state of LEDs on the module.

Writes to these fields are non-postable cycles, and the resulting message is a postable cycle. When receiving one of these writes, the root port performs the following:

- Changes the state in the register.
- Generates a completion into the upstream queue
- Formulates a message for the downstream port if the field is written to regardless of if the field changed.

- Generates the message on the downstream port
- When the last message of a command is transmitted, sets SLSTS.CCE (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 58h:Bit 4) to indicate the command has completed. If SLCTL.CCE and SLCTL.HPE (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 58h:Bit 5) are set, the root port generates an interrupt.

The command completed register (SLSTS.CC) applies only to commands issued by software to control the Attention Indicator (SLCTL.AIC), Power Indicator (SLCTL.PIC), or Power Controller (SLCTL.PCC). However, writes to other parts of the Slot Control Register would invariably end up writing to the indicators and power controller fields. Hence, any write to the Slot Control Register is considered a command and if enabled, will result in a command complete interrupt. The only exception to this rule is a write to disable the command complete interrupt which will not result in a command complete interrupt.

A single write to the Slot Control register is considered to be a single command, and, hence, receives a single command complete, even if the write affects more than one field in the Slot Control Register.

3.2.5.3 Attention Button Detection

When an attached device is ejected, an attention button could be pressed by the user. This attention button press will result in a the PCI Express* message "Attention_Button_Pressed" from the device. Upon receiving this message, the root port will set SLSTS.ABP (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 5Ah:Bit 0).

If SLCTL.ABE (D28:F0/F1/F2/F3/F4/F5:Offset 58h:bit 0) and SLCTL.HPE (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 58h:Bit 5) are set, the Hot-Plug controller will also generate an interrupt. The interrupt is generated on an edge-event. For example, if SLSTS.ABP is already set, a new interrupt will not be generated.

3.2.5.4 SMI/SCI Generation

Interrupts for Hot-Plug events are not supported on legacy operating systems. To support Hot-Plug on n on-PCI Express aware operating systems, Hot-Plug events can be routed to generate SCI. To generate SCI, MPC.HPCE (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset D8h:Bit 30) must be set. When set, enabled Hot-Plug events will cause SMSCS.HPCS (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset DCh:Bit 30) to be set.

Additionally, BIOS workarounds for Hot-Plug can be supported by setting MPC.HPME (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset D8h:Bit 1). When this bit is set, Hot-Plug events can cause SMI status bits in SMSCS to be set. Supported Hot-Plug events and their corresponding SMSCS bit are:

- Command Completed – SCSCS.HPCCM (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset DCh:Bit 3)
- Presence Detect Changed – SMSCS.HPPDM (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset DCh:Bit 1)
- Attention Button Pressed – SMSCS.HPABM (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset DCh:Bit 2)
- Link Active State Changed – SMSCS.HPLAS (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset DCh:Bit 4)

When any of these bits are set, SMI# will be generated. These bits are set regardless of whether interrupts or SCI is enabled for Hot-Plug events. The SMI# may occur concurrently with an interrupt or SCI.

3.3 Gigabit Ethernet Controller (B0:D25:F0)

Intel® Xeon® Processor D-1500 Product Family integrates a Gigabit Ethernet (GbE) controller. The integrated GbE controller is compatible with the Intel® Ethernet Network Connection i217LM/V Platform LAN Connect device. The integrated GbE controller provides two interfaces for 10/100/1000 Mb/s and manageability operation:

- Based on PCI Express* – A high-speed SerDes interface using PCI Express electrical signaling at half speed while keeping the custom logical protocol for active state operation mode.
- System Management Bus (SMBus) SMLink – A low speed connection for low power state mode for manageability communication only. The frequency of this connection can be configured to one of three different speeds (100 kHz, 400 kHz or 1 MHz). At this low power state mode the Ethernet link speed is reduced to 10 Mb/s.

Note: The SMBus Specification Version 2.0 defines a maximum bus frequency of 100 kHz. Speeds faster than this are not SMBus compliant and are used by Intel to support higher bandwidth manageability communication in the Sx states.

The Intel Ethernet Network Connection i217LM/V only runs at a speed of 1250 Mb/s, which is 1/2 of the 2.5 Gb/s PCI Express* frequency. Each of the fixed signal PCI Express root ports in Intel® Xeon® Processor D-1500 Product Family have the ability to run at the 1250 Mb/s rate. There is no need to implement a mechanism to detect that the Platform LAN Device is connected. The port configuration (if any), attached to the Platform LAN Device, is pre-loaded from the NVM. The selected port adjusts the transmitter to run at the 1250 Mb/s rate and does not need to be PCI Express compliant.

Note: PCIe validation tools cannot be used for electrical validation of this interface; however, PCIe layout rules apply for on-board routing.

The integrated GbE controller operates at full-duplex at all supported speeds or half-duplex at 10/100 Mb/s. It also adheres to the *IEEE 802.3x Flow Control Specification.*

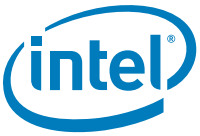
Note: GbE operation (1000 Mb/s) is only supported in S0 mode. In Sx modes, SMBus is the only active bus and is used to support manageability/remote wake-up functionality.

The integrated GbE controller provides a system interface using a PCI Express function. A full memory-mapped or I/O-mapped interface is provided to the software, along with DMA mechanisms for high performance data transfer.

The integrated GbE controller features are:

- Network Features
  - Compliant with the 1 Gb/s Ethernet 802.3, 802.3u, 802.3z, 802.3ab specifications
  - Multi-speed operation: 10/100/1000 Mb/s
  - Full-duplex operation at 10/100/1000 Mb/s: Half-duplex at 10/100 Mb/s
  - Flow control support compliant with the 802.3X specification as well as the specific operation of asymmetrical flow control defined by 802.3z

  - VLAN support compliant with the 802.3q specification
  - MAC address filters: perfect match unicast filters; multicast hash filtering, broadcast filter and promiscuous mode
  - PCI Express/SMBus interface to GbE PHYs
- Host Interface Features
  - 64-bit address master support for systems using more than 4 GB of physical memory
  - Programmable host memory receive buffers (256 Bytes to 16 KB)
  - Intelligent interrupt generation features to enhance driver performance
  - Descriptor ring management hardware for transmit and receive
  - Software controlled reset (resets everything except the configuration space)
  - Message Signaled Interrupts
- Performance Features
  - Configurable receive and transmit data FIFO, programmable in 1 KB increments
  - TCP segmentation capability compatible with Windows NT* 5.x off loading features
  - Fragmented UDP checksum offload for packet reassembly
  - IPv4 and IPv6 checksum offload support (receive, transmit, and TCP segmentation offload)
  - Split header support to eliminate payload copy from user space to host space
  - Receive Side Scaling (RSS) with two hardware receive queues
  - Supports 9018 bytes of jumbo packets
  - Packet buffer size
  - LinkSec offload compliant with 802.3ae specification
  - TimeSync offload compliant with 802.1as specification
- Virtualization Technology Features
  - Warm function reset – function level reset (FLR)
  - VMDq1
- Power Management Features
  - Magic Packet* wake-up enable with unique MAC address
  - ACPI register set and power down functionality supporting D0 and D3 states
  - Full wake up support (APM, ACPI)
  - MAC power down at Sx, DMoff with and without WoL
  - Auto connect battery saver at S0 no link and Sx no link
  - Energy Efficient Ethernet (EEE) support
  - Latency Tolerance Reporting (LTR)
  - ARP and ND proxy support through LAN Connected Device proxy



3.3.1 GbE PCI Express* Bus Interface

The GbE controller has a PCI Express interface to the host processor and host memory. The following sections detail the bus transactions.

3.3.1.1 Transaction Layer

The upper layer of the host architecture is the transaction layer. The transaction layer connects to the device GbE controller using an implementation specific protocol. Through this GbE controller-to-transaction-layer protocol, the application-specific parts of the device interact with the subsystem and transmit and receive requests to or from the remote agent, respectively.

3.3.1.2 Data Alignment

3.3.1.2.1 4-KB Boundary

PCI requests must never specify an address/length combination that causes a memory space access to cross a 4 KB boundary. It is hardware's responsibility to break requests into 4 KB-aligned requests (if needed). This does not pose any requirement on software. However, if software allocates a buffer across a 4-KB boundary, hardware issues multiple requests for the buffer. Software should consider aligning buffers to a 4-KB boundary in cases where it improves performance.

The alignment to the 4-KB boundaries is done by the GbE controller. The transaction layer does not do any alignment according to these boundaries.

3.3.1.2.2 64 Bytes

PCI requests are 128 bytes or less and are aligned to make better use of memory controller resources. Writes, however, can be on any boundary and can cross a 64-byte alignment boundary.

3.3.1.3 Configuration Request Retry Status

The integrated GbE controller might have a delay in initialization due to an NVM read. If the NVM configuration read operation is not completed and the device receives a configuration request, the device responds with a configuration request retry completion status to terminate the request, and thus effectively stalls the configuration request until such
time that the sub-system has completed local initialization and is ready to communicate with the host.

3.3.2 Error Events and Error Reporting

3.3.2.1 Data Parity Error

The PCI host bus does not provide parity protection, but it does forward parity errors from bridges. The integrated GbE controller recognizes parity errors through the internal bus interface and sets the *Parity Error* bit in PCI configuration space. If parity errors are enabled in configuration space, a system error is indicated on the PCI host bus. The offending cycle with a parity error is dropped and not processed by the integrated GbE controller.

3.3.2.2 Completion with Unsuccessful Completion Status

A completion with unsuccessful completion status (any status other than 000) is dropped and not processed by the integrated GbE controller. Furthermore, the request that corresponds to the unsuccessful completion is not retried. When this unsuccessful completion status is received, the *System Error* bit in the PCI configuration space is set. If the system errors are enabled in configuration space, a system error is indicated on the PCI host bus.

3.3.3 Ethernet Interface

The integrated GbE controller provides a complete CSMA/CD function supporting IEEE 802.3 (10 Mb/s), 802.3u (100 Mb/s) implementations. It also supports the IEEE 802.3z and 802.3ab (1000 Mb/s) implementations. The device performs all of the functions required for transmission, reception, and collision handling called out in the standards.

The mode used to communicate between Intel® Xeon® Processor D-1500 Product Family and the Intel® Ethernet Network Connection i217LM/V Platform LAN Connect Device supports 10/100/1000 Mb/s operation, with both half- and full-duplex operation at 10/100 Mb/s, and full-duplex operation at 1000 Mb/s.

3.3.3.1 Intel® Ethernet Network Connection i217LM/V Platform LAN Connect Device Interface

The integrated GbE controller and the Intel® Ethernet Network Connection i217LM/V Platform LAN Connect Device communicate through the PCIe and SMLink interfaces. All integrated GbE controller configuration is performed using device control registers mapped into system memory or I/O space. The Platform LAN Connect Device is configured using the PCI Express* or SMBus interface.

The integrated GbE controller supports various modes as listed in Table 3-4.

Table 3-4. LAN Mode Support

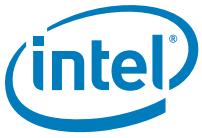
Mode	System State	Interface Active	Connections
Normal 10/100/1000 Mb/s	S0	PCI Express or SMLink[1]	Intel Ethernet Network Connection i217LM/V
Manageability and Remote Wake-up	Sx	SMLink	Intel Ethernet Network Connection i217LM/V

Notes:
1. GbE operation is not supported in Sx states.

3.3.4 PCI Power Management

The integrated GbE controller supports the Advanced Configuration and Power Interface (ACPI) specification as well as Advanced Power Management (APM). This enables the network-related activity (using an internal host wake signal) to wake up the host.

The integrated GbE controller contains power management registers for PCI and supports D0 and D3 states. PCIe* transactions are only allowed in the D0 state, except for host accesses to the integrated GbE controller's PCI configuration registers.



3.3.4.1 Wake Up

The integrated GbE controller supports two types of wake-up mechanisms:

1. Advanced Power Management (APM) Wake Up
2. ACPI Power Management Wake Up

Both mechanisms use an internal logic signal to wake the system up. The wake-up steps are as follows:

1. Host wake event occurs (packet is not delivered to host).
2. The Platform LAN Connect Device receives a WoL packet/link status change.
3. The Platform LAN Connect Device sends a wake indication to Intel® Xeon® Processor D-1500 Product Family (this requires the WAKELAN_N pin from the Intel® Ethernet Network Connection i217LM/V Platform LAN Connect Device to be connected to Intel® Xeon® Processor D-1500 Product Family GPIO27 pin.
4. The Platform LAN Connect Device wakes up the integrated GbE controller using an SMBus message on SMLink.
5. The integrated GbE controller sets the *PME_STATUS* bit.
6. System wakes from Sx state to S0 state.
7. The host LAN function is transitioned to D0.
8. The host clears the *PME_STATUS* bit.

3.3.4.1.1 Advanced Power Management Wake Up

Advanced Power Management Wake Up or APM Wake Up was previously known as Wake on LAN (WoL). It is a feature that has existed in the 10/100 Mb/s NICs for several generations. The basic premise is to receive a broadcast or unicast packet with an explicit data pattern and then to assert a signal to wake up the system. In earlier generations, this was accomplished by using a special signal that ran across a cable to a defined connector on the motherboard. The NIC would assert the signal for approximately 50 ms to signal a wake up. The integrated GbE controller uses (if configured to) an in-band PM_PME message for this.

At power up, the integrated GbE controller reads the *APM Enable* bits from the NVM PCI Init Control Word into the APM Enable (APME) bits of the Wake Up Control (WUC) register. These bits control enabling of APM wake up.

When APM wake up is enabled, the integrated GbE controller checks all incoming packets for Magic Packets.

Once the integrated GbE controller receives a matching Magic Packet, it:

- Sets the Magic Packet *Received* bit in the Wake Up Status (WUS) register.
- Sets the *PME_Status* bit in the Power Management Control/Status Register (PMCSR).

APM wake up is supported in all power states and only disabled if a subsequent NVM read results in the *APM Wake Up* bit being cleared or the software explicitly writes a 0b to the *APM Wake Up* (APM) bit of the WUC register.

Note: APM wake up settings will be restored to NVM default by Intel® Xeon® Processor D-1500 Product Family when LAN connected Device (PHY) power is turned off and subsequently restored. Some example host WoL flows are:

- When system transitions to G3 after WoL is disabled from the BIOS, APM host WoL would get enabled.
- Anytime power to the LAN Connected Device (PHY) is cycled while in S4/S5 after WoL is disabled from the BIOS, APM host WoL would get enabled. Anytime power to the LAN Connected Device (PHY) is cycled while in S3, APM host WoL configuration is lost.

3.3.4.1.2 ACPI Power Management Wake Up

The integrated GbE controller supports ACPI Power Management based Wake ups. It can generate system wake-up events from three sources:

- Receiving a Magic Packet*.
- Receiving a Network Wake Up Packet.
- Detecting a link change of state.

Activating ACPI Power Management Wakeup requires the following steps:

- The software device driver programs the Wake Up Filter Control (WUFC) register to indicate the packets it needs to wake up from and supplies the necessary data to the IPv4 Address Table (IP4AT) and the Flexible Filter Mask Table (FFMT), Flexible Filter Length Table (FFLT), and the Flexible Filter Value Table (FFVT). It can also set the *Link Status Change Wake Up Enable* (LNKC) bit in the Wake Up Filter Control (WUFC) register to cause wake up when the link changes state.
- The operating system (at configuration time) writes a 1b to the *PME_EN* bit of the Power Management Control/Status Register (PMCSR.8).

Normally, after enabling wake up, the operating system writes a 11b to the lower two bits of the PMCSR to put the integrated GbE controller into low-power mode.

Once wake up is enabled, the integrated GbE controller monitors incoming packets, first filtering them according to its standard address filtering method, then filtering them with all of the enabled wake-up filters. If a packet passes both the standard address filtering and at least one of the enabled wake-up filters, the integrated GbE controller:

- Sets the *PME_Status* bit in the PMCSR
- Sets one or more of the *Received* bits in the Wake Up Status (WUS) register. (More than one bit is set if a packet matches more than one filter.)

If enabled, a link state change wake up causes similar results, setting the *Link Status Changed* (LNKC) bit in the Wake Up Status (WUS) register when the link goes up or down.

After receiving a wake-up packet, the integrated GbE controller ignores any subsequent wake-up packets until the software device driver clears all of the *Received* bits in the Wake Up Status (WUS) register. It also ignores link change events until the software device driver clears the *Link Status Changed* (LNKC) bit in the Wake Up Status (WUS) register.

Note: ACPI wake up settings are not preserved when the LAN Connected Device (PHY) power is turned off and subsequently restored. Some example host WoL flows are:

- Anytime power to the LAN Connected Device (PHY) is cycled while in S4, ACPI host WoL configuration is lost.

3.3.5 Configurable LEDs

The integrated GbE controller supports three controllable and configurable LEDs that are driven from the Intel Ethernet Network Connection i217LM/V Platform LAN Connect Device. Each of the three LED outputs can be individually configured to select the particular event, state, or activity that is indicated on that output. In addition, each LED can be individually configured for output polarity as well as for blinking versus non-blinking (steady-state) indication.

The configuration for LED outputs is specified using the LEDCTL register. Furthermore, the hardware-default configuration for all the LED outputs, can be specified using NVM fields; thereby, supporting LED displays configurable to a particular OEM preference.

Each of the three LEDs might be configured to use one of a variety of sources for output indication. The MODE bits control the LED source:

- LINK_100/1000 is asserted when link is established at either 100 or 1000 Mb/s.
- LINK_10/1000 is asserted when link is established at either 10 or 1000 Mb/s.
- LINK_UP is asserted when any speed link is established and maintained.
- ACTIVITY is asserted when link is established and packets are being transmitted or received.
- LINK/ACTIVITY is asserted when link is established AND there is NO transmit or receive activity.
- LINK_10 is asserted when a 10 Mb/s link is established and maintained.
- LINK_100 is asserted when a 100 Mb/s link is established and maintained.
- LINK_1000 is asserted when a 1000 Mb/s link is established and maintained.
- FULL_DUPLEX is asserted when the link is configured for full duplex operation.
- COLLISION is asserted when a collision is observed.
- PAUSED is asserted when the device's transmitter is flow controlled.
- LED_ON is always asserted; LED_OFF is always de-asserted.

The *IVRT* bits enable the LED source to be inverted before being output or observed by the blink-control logic. LED outputs are assumed to normally be connected to the negative side (cathode) of an external LED.

The *BLINK* bits control whether the LED should be blinked while the LED source is asserted, and the blinking frequency (either 200 ms on and 200 ms off or 83 ms on and 83 ms off). The blink control can be especially useful for ensuring that certain events, such as ACTIVITY indication, cause LED transitions, which are sufficiently visible to a human eye. The same blinking rate is shared by all LEDs.

3.3.6 Function Level Reset Support (FLR)

The integrated GbE controller supports FLR capability. FLR capability can be used in conjunction with Intel® Virtualization Technology. FLR allows an operating system in a Virtual Machine to have complete control over a device, including its initialization, without interfering with the rest of the platform. The device provides a software interface that enables the operating system to reset the entire device as if a PCI reset was asserted.

3.3.6.1 FLR Steps

3.3.6.1.1 FLR Initialization

1. FLR is initiated by software by writing a 1b to the *Initiate FLR* bit.
2. All subsequent requests targeting the function are not claimed and will be master aborted immediately on the bus. This includes any configuration, I/O or memory cycles. However, the function will continue to accept completions targeting the function.

3.3.6.1.2 FLR Operation

Function resets all configuration, I/O, and memory registers of the function except those indicated otherwise and resets all internal states of the function to the default or initial condition.

3.3.6.1.3 FLR Completion

The *Initiate FLR* bit is reset (cleared) when the FLR reset completes. This bit can be used to indicate to the software that the FLR reset completed.

Note: From the time the *Initiate FLR* bit is written to 1b, software must wait at least 100 ms before accessing the function.

3.4 Low Pin Count (LPC) Bridge (with System and Management Functions) (D31:F0)

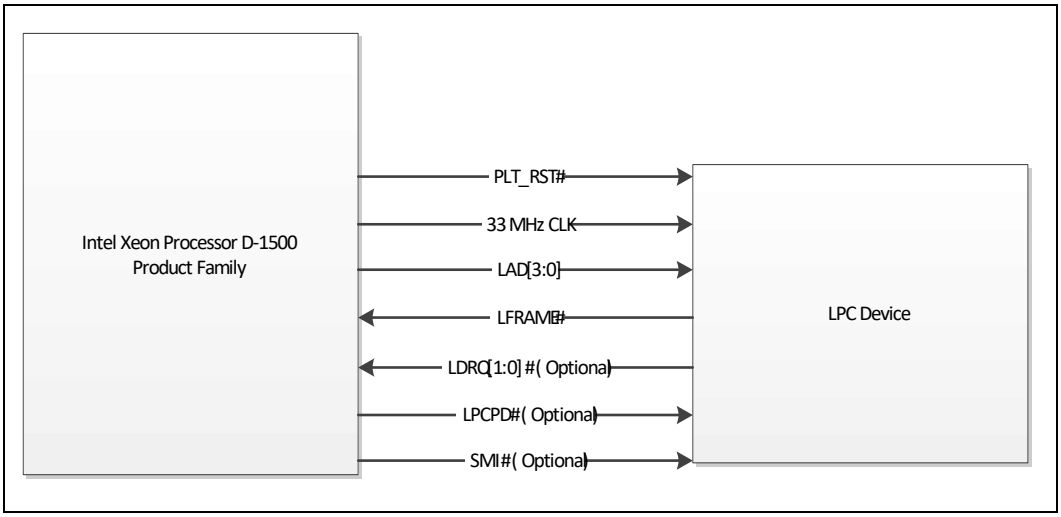
The LPC bridge function of Intel® Xeon® Processor D-1500 Product Family resides in PCI D31:F0. In addition to the LPC bridge function, D31:F0 contains other functional units including DMA, Interrupt controllers, Timers, Power Management, System Management, GPIO, and RTC. In this chapter, registers and functions associated with other functional units (power management, GPIO, USB, and so on) are described in their respective sections.

Note: The LPC bridge cannot be configured as a subtractive decode agent.

3.4.1 LPC Interface

Intel® Xeon® Processor D-1500 Product Family implements an LPC interface as described in the *Low Pin Count Interface Specification,* Revision 1.1. The LPC interface to Intel® Xeon® Processor D-1500 Product Family is shown in Figure 3-2.
Intel® Xeon® Processor D-1500 Product Family implements all of the signals that are shown as optional, but peripherals are not required to do so.

Figure 3-2. LPC Interface Diagram



3.4.1.1 LPC Cycle Types

Intel® Xeon® Processor D-1500 Product Family implements all of the cycle types described in the *Low Pin Count Interface Specification,* Revision 1.1. Table 3-5 shows the cycle types supported by Intel® Xeon® Processor D-1500 Product Family.

Table 3-5. LPC Cycle Types Supported

Cycle Type	Comment
Memory Read	1 byte only. (See Note 1 below)
Memory Write	1 byte only. (See Note 1 below)
I/O Read	1 byte only. Intel® Xeon® Processor D-1500 Product Family breaks up 16-bit and 32-bit processor cycles into multiple 8-bit transfers.
I/O Write	1 byte only. Intel® Xeon® Processor D-1500 Product Family breaks up 16-bit and 32-bit processor cycles into multiple 8-bit transfers.
DMA Read	Can be 1 or 2 bytes
DMA Write	Can be 1 or 2 bytes
Bus Master Read	Can be 1, 2 or 4 bytes. (See Note 2 below)
Bus Master Write	Can be 1, 2 or 4 bytes. (See Note 2 below)

Notes:

1. Intel® Xeon® Processor D-1500 Product Family provides a single generic memory range (LGMR) for decoding memory cycles and forwarding them as LPC Memory cycles on the LPC bus. The LGMR memory decode range is 64 KB in size and can be defined as being anywhere in the 4 GB memory space. This range needs to be configured by BIOS during POST to provide the necessary memory resources. BIOS should advertise the LPC Generic Memory Range as Reserved to the OS in order to avoid resource conflict. For larger transfers, Intel® Xeon® Processor D-1500 Product Family performs multiple 8-bit transfers. If the cycle is not claimed by any peripheral, it is subsequently aborted, and Intel® Xeon® Processor D-1500 Product Family returns a value of all 1s to the processor. This is done to maintain compatibility with ISA memory cycles where pull-up resistors would keep the bus high if no device responds.
2. Bus Master Read or Write cycles must be naturally aligned. For example, a 1-byte transfer can be to any address. However, the 2-byte transfer must be word-aligned (that is, with an address where A0=0). A DWord transfer must be DWord-aligned (that is, with an address where A1 and A0 are both 0).

3.4.1.2 Start Field Definition

Table 3-6. Start Field Bit Definitions

Bits[3:0] Encoding	Definition
0000	Start of cycle for a generic target
0010	Grant for bus master 0
0011	Grant for bus master 1
1111	Stop/Abort: End of a cycle for a target.

Note: All other encodings are RESERVED.

3.4.1.3 Cycle Type / Direction (CYCTYPE + DIR)

Intel® Xeon® Processor D-1500 Product Family always drives Bit 0 of this field to 0. Peripherals running bus master cycles must also drive Bit 0 to 0. Table 3-7 shows the valid bit encodings.

Table 3-7. Cycle Type Bit Definitions

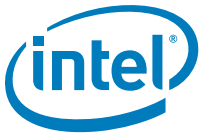
Bits[3:2]	Bit1	Definition
00	0	I/O Read
00	1	I/O Write
01	0	Memory Read
01	1	Memory Read
10	0	DMA Read
10	1	DMA Write
11	x	Reserved. If a peripheral performing a bus master cycle generates this value, Intel® Xeon® Processor D-1500 Product Family aborts the cycle.

3.4.1.4 Size

Bits[3:2] are reserved. Intel® Xeon® Processor D-1500 Product Family always drives them to 00. Peripherals running bus master cycles are also supposed to drive 00 for Bits 3:2; however, Intel® Xeon® Processor D-1500 Product Family ignores those bits. Bits[1:0] are encoded as listed in Table 3-8.

Table 3-8. Transfer Size Bit Definition

Bits[1:0]	Size
00	8-bit transfer (1 byte)
01	16-bit transfer (2 bytes)
10	Reserved. Intel® Xeon® Processor D-1500 Product Family never drives this combination. If a peripheral running a bus master cycle drives this combination, Intel® Xeon® Processor D-1500 Product Family may abort the transfer.
11	32-bit transfer (4 bytes)



3.4.1.5 SYNC

Valid values for the SYNC field are shown in Table 3-9.

Table 3-9. SYNC Bit Definition

Bits[3:0]	Indication
0000	**Ready:** SYNC achieved with no error. For DMA transfers, this also indicates DMA request de-assertion and no more transfers desired for that channel.
0101	**Short Wait:** Part indicating wait-states. For bus master cycles, Intel® Xeon® Processor D-1500 Product Family does not use this encoding. Instead, Intel® Xeon® Processor D-1500 Product Family uses the Long Wait encoding (see next encoding below).
0110	**Long Wait:** Part indicating wait-states, and many wait-states will be added. This encoding driven by Intel® Xeon® Processor D-1500 Product Family for bus master cycles, rather than the Short Wait (0101).
1001	**Ready More (Used only by peripheral for DMA cycle):** SYNC achieved with no error and more DMA transfers desired to continue after this transfer. This value is valid only on DMA transfers and is not allowed for any other type of cycle.
1010	**Error:** Sync achieved with error. This is generally used to replace the SERR# or IOCHK# signal on the PCI/ISA bus. It indicates that the data is to be transferred, but there is a serious error in this transfer. For DMA transfers, this not only indicates an error, but also indicates DMA request de-assertion and no more transfers desired for that channel.

Notes:
1. All other combinations are RESERVED.
2. If the LPC controller receives any SYNC returned from the device other than short (0101), long wait (0110), or ready (0000) when running a FWH cycle, indeterminate results may occur. A FWH device is not allowed to assert an Error SYNC.

3.4.1.6 SYNC Time-Out

There are several error cases that can occur on the LPC interface. Intel® Xeon® Processor D-1500 Product Family responds as defined in Section 4.2.1.9 of the *Low Pin Count Interface Specification*, Revision 1.1 to the stimuli described therein. There may be other peripheral failure conditions; however, these are not handled by Intel® Xeon® Processor D-1500 Product Family.

3.4.1.7 SYNC Error Indication

Intel® Xeon® Processor D-1500 Product Family responds as defined in Section 4.2.1.10 of the *Low Pin Count Interface Specification,* Revision 1.1.

Upon recognizing the SYNC field indicating an error, Intel® Xeon® Processor D-1500 Product Family treats this as a SERR by reporting this into the Device 31 Error Reporting Logic.

3.4.1.8 LFRAME# Usage

Intel® Xeon® Processor D-1500 Product Family follows the usage of LFRAME# as defined in the *Low Pin Count Interface Specification,* Revision 1.1.

Intel® Xeon® Processor D-1500 Product Family performs an abort for the following cases (possible failure cases):

- Intel® Xeon® Processor D-1500 Product Family starts a Memory, I/O, or DMA cycle, but no device drives a valid SYNC after four consecutive clocks.
- Intel® Xeon® Processor D-1500 Product Family starts a Memory, I/O, or DMA cycle, and the peripheral drives an invalid SYNC pattern.
- A peripheral drives an illegal address when performing bus master cycles.

- A peripheral drives an invalid value.

3.4.1.9 I/O Cycles

For I/O cycles targeting registers specified in Intel® Xeon® Processor D-1500 Product Family's decode ranges, Intel® Xeon® Processor D-1500 Product Family performs I/O cycles as defined in the *Low Pin Count Interface Specification,* Revision 1.1. These are 8-bit transfers. If the processor attempts a 16-bit or 32-bit transfer, Intel® Xeon® Processor D-1500 Product Family breaks the cycle up into multiple 8-bit transfers to consecutive I/O addresses.

Note: If the cycle is not claimed by any peripheral (and subsequently aborted), Intel® Xeon® Processor D-1500 Product Family returns a value of all 1s (FFh) to the processor. This is to maintain compatibility with ISA I/O cycles where pull-up resistors would keep the bus high if no device responds.

3.4.1.10 Bus Master Cycles

Intel® Xeon® Processor D-1500 Product Family supports Bus Master cycles and requests (using LDRQ#) as defined in the *Low Pin Count Interface Specification,* Revision 1.1. Intel® Xeon® Processor D-1500 Product Family has two LDRQ# inputs, and thus supports two separate bus master devices. It uses the associated START fields for Bus Master 0 (0010b) or Bus Master 1 (0011b).

Note: Intel® Xeon® Processor D-1500 Product Family does not support LPC Bus Masters performing I/O cycles. LPC Bus Masters should only perform memory read or memory write cycles.

3.4.1.11 LPC Power Management

LPCPD# Protocol

Same timings as for SUS_STAT#. Upon driving SUS_STAT# low, LPC peripherals drive LDRQ# low or tri-state it. Intel® Xeon® Processor D-1500 Product Family shuts off the LDRQ# input buffers. After driving SUS_STAT# active, Intel® Xeon® Processor D-1500 Product Family drives LFRAME# low, and tri-states (or drives low) LAD[3:0].

Note: The *Low Pin Count Interface Specification,* Revision 1.1 defines the LPCPD# protocol where there is at least 30 µs from LPCPD# assertion to LRST# assertion. This specification explicitly states that this protocol only applies to entry/exit of low power states which does not include asynchronous reset events. Intel® Xeon® Processor D-1500 Product Family asserts both SUS_STAT# (connects to LPCPD#) and PLTRST# (connects to LRST#) at the same time during a global reset. This is not inconsistent with the LPC LPCPD# protocol.

3.4.1.12 Configuration and Intel® Xeon® Processor D-1500 Product Family Implications

LPC I/F Decoders

To allow the I/O cycles and memory mapped cycles to go to the LPC interface, Intel® Xeon® Processor D-1500 Product Family includes several decoders. During configuration, Intel® Xeon® Processor D-1500 Product Family must be programmed with the same decode ranges as the peripheral. The decoders are programmed using the D 31:F0 configuration space.

Note: Intel® Xeon® Processor D-1500 Product Family cannot accept PCI write cycles from PCI-to-PCI bridges or devices with similar characteristics (specifically those with a "Retry Read" feature which is enabled) to an LPC device if there is an outstanding LPC read cycle towards the same PCI device or bridge. These cycles are not part of normal system operation, but may be encountered as part of platform validation testing using custom test fixtures.

Bus Master Device Mapping and START Fields

Bus Masters must have a unique START field. In the case of Intel® Xeon® Processor D-1500 Product Family that supports two LPC bus masters, it drives 0010 for the START field for grants to Bus Master 0 (requested using LDRQ0#) and 0011 for grants to Bus Master 1 (requested using LDRQ1#.). Thus, no registers are needed to configure the START fields for a particular bus master.

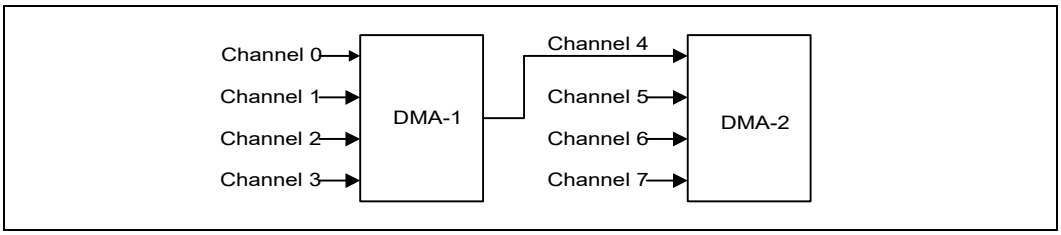
3.5 DMA Operation (D31:F0)

Intel® Xeon® Processor D-1500 Product Family supports LPC DMA using Intel® Xeon® Processor D-1500 Product Family's DMA controller. The DMA controller has registers that are fixed in the lower 64 KB of I/O space. The DMA controller is configured using registers in the PCI configuration space. These registers allow configuration of the channels for use by LPC DMA.

The DMA circuitry incorporates the functionality of two 8237 DMA controllers with seven independently programmable channels (Figure 3-3). DMA Controller 1 (DMA-1) corresponds to DMA Channels 0–3 and DMA Controller 2 (DMA-2) corresponds to Channels 5–7. DMA Channel 4 is used to cascade the two controllers and defaults to cascade mode in the DMA Channel Mode (DCM) Register. Channel 4 is not available for any other purpose. In addition to accepting requests from DMA slaves, the DMA controller also responds to requests that software initiates. Software may initiate a DMA service request by setting any bit in the DMA Channel Request Register to a 1.

Floppy disk is not supported (or validated) in this Intel® Xeon® Processor D-1500 Product Family.

Figure 3-3. Intel® Xeon® Processor D-1500 Product Family DMA Controller



Each DMA channel is hardwired to the compatible settings for DMA device size: Channels [3:0] are hardwired to 8-bit, count-by-bytes transfers, and Channels [7:5] are hardwired to 16-bit, count-by-words (address shifted) transfers.

Intel® Xeon® Processor D-1500 Product Family provides 24-bit addressing in compliance with the ISA-Compatible specification. Each channel includes a 16-bit ISA-Compatible Current Register which holds the sixteen least-significant bits of the 24-bit address, an ISA-Compatible Page Register which contains the eight next most significant bits of address.

The DMA controller also features refresh address generation, and auto-initialization following a DMA termination.

3.5.1 Channel Priority

For priority resolution, the DMA consists of two logical channel groups: Channels 0–3 and Channels 4–7. Each group may be in either fixed or rotate mode, as determined by the DMA Command Register.

DMA I/O slaves normally assert their DREQ line to arbitrate for DMA service. However, a software request for DMA service can be presented through each channel's DMA Request Register. A software request is subject to the same prioritization as any hardware request. See the detailed register description for Request Register programming information in Section 7.2.

3.5.1.1 Fixed Priority

The initial fixed priority structure is as follows:

High priority	Low priority
0, 1, 2, 3	5, 6, 7

The fixed priority ordering is 0, 1, 2, 3, 5, 6, and 7. In this scheme, channel 0 has the highest priority, and channel 7 has the lowest priority. Channels [3:0] of DMA-1 assume the priority position of channel 4 in DMA-2, thus taking priority over Channels 5, 6, and 7.

3.5.1.2 Rotating Priority

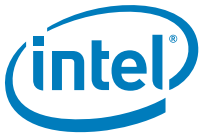
Rotation allows for "fairness" in priority resolution. The priority chain rotates so that the last channel serviced is assigned the lowest priority in the channel group (0–3, 5–7).

Channels 0–3 rotate as a group of 4. They are always placed between Channel 5 and Channel 7 in the priority list.

Channel 5–7 rotate as part of a group of 4. That is, Channels (5–7) form the first three positions in the rotation, while Channel Group (0–3) comprises the fourth position in the arbitration.

3.5.2 Address Compatibility Mode

When the DMA is operating, the addresses do not increment or decrement through the High and Low Page Registers. Therefore, if a 24-bit address is 01FFFFh and increments, the next address is 010000h, not 020000h. Similarly, if a 24-bit address is 020000h and decrements, the next address is 02FFFFh, not 01FFFFh. However, when the DMA is operating in 16-bit mode, the addresses still do not increment or decrement through the High and Low Page Registers but the page boundary is now 128 K. Therefore, if a 24-bit address is 01FFFEh and increments, the next address is 000000h, not 0100000h. Similarly, if a 24-bit address is 020000h and decrements, the next address is 03FFFEh, not 02FFFEh. This is compatible with the 8237 and Page Register implementation used in the PC-AT. This mode is set after CPURST is valid.



3.5.3 Summary of DMA Transfer Sizes

Table 3-10 lists each of the DMA device transfer sizes. The column labeled "Current Byte/Word Count Register" indicates that the register contents represents either the number of bytes to transfer or the number of 16-bit words to transfer. The column labeled "Current Address Increment/Decrement" indicates the number added to or taken from the Current Address register after each DMA transfer cycle. The DMA Channel Mode Register determines if the Current Address Register will be incremented or decremented.

3.5.3.1 Address Shifting When Programmed for 16-Bit I/O Count by Words

Table 3-10. DMA Transfer Size

DMA Device Date Size And Word Count	Current Byte/Word Count Register	Current Address Increment / Decrement
8-Bit I/O, Count By Bytes	Bytes	1
16-Bit I/O, Count By Words (Address Shifted)	Words	1

Intel® Xeon® Processor D-1500 Product Family maintains compatibility with the implementation of the DMA in the PC AT that used the 8237. The DMA shifts the addresses for transfers to/from a 16-bit device count-by-words.

Note: The least significant bit of the Low Page Register is dropped in 16-bit shifted mode. When programming the Current Address Register (when the DMA channel is in this mode), the Current Address must be programmed to an even address with the address value shifted right by one bit.

The address shifting is shown in Table 3-11.

Table 3-11. Address Shifting in 16-Bit I/O DMA Transfers

Output Address	8-Bit I/O Programmed Address (Ch 0–3)	16-Bit I/O Programmed Address (Ch 5–7) (Shifted)
A0 A[16:1] A[23:17]	A0 A[16:1] A[23:17]	0 A[15:0] A[23:17]

Note: The least significant bit of the Page Register is dropped in 16-bit shifted mode.

3.5.4 Autoinitialize

By programming a bit in the DMA Channel Mode Register, a channel may be set up as an autoinitialize channel. When a channel undergoes autoinitialization, the original values of the Current Page, Current Address and Current Byte/Word Count Registers are automatically restored from the Base Page, Address, and Byte/Word Count Registers of that channel following Terminal Count (TC). The Base Registers are loaded simultaneously with the Current Registers by the microprocessor when the DMA channel is programmed and remain unchanged throughout the DMA service. The mask bit is not set when the channel is in autoinitialize. Following autoinitialize, the channel is ready to perform another DMA service, without processor intervention, as soon as a valid DREQ is detected.

3.5.5 Software Commands

There are three additional special software commands that the DMA controller can execute. The three software commands are:

- Clear Byte Pointer Flip-Flop
- Master Clear
- Clear Mask Register

They do not depend on any specific bit pattern on the data bus.

3.6 Low Pin Count (LPC) DMA

DMA on LPC is handled through the use of the LDRQ# lines from peripherals and special encodings on LAD[3:0] from the host. Single, Demand, Verify, and Increment modes are supported on the LPC interface. Channels 0–3 are 8-bit channels. Channels 5–7 are 16-bit channels. Channel 4 is reserved as a generic bus master request.

3.6.1 Asserting DMA Requests

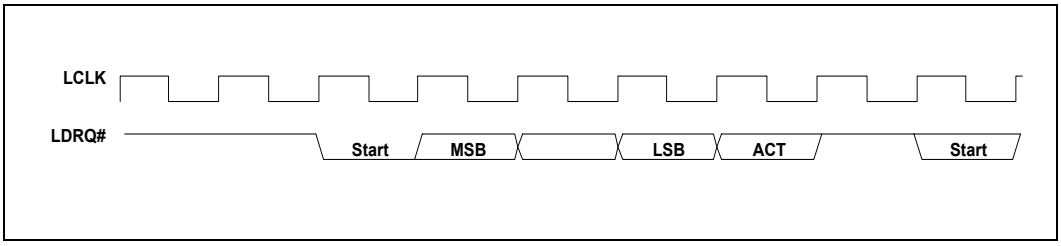
Peripherals that need DMA service encode their requested channel number on the LDRQ# signal. To simplify the protocol, each peripheral on the LPC I/F has its own dedicated LDRQ# signal (they may not be shared between two separate peripherals). Intel® Xeon® Processor D-1500 Product Family has two LDRQ# inputs, allowing at least two devices to support DMA or bus mastering.

LDRQ# is synchronous with LCLK (PCI clock). As shown in Figure 3-4, the peripheral uses the following serial encoding sequence:

- Peripheral starts the sequence by asserting LDRQ# low (start bit). LDRQ# is high during idle conditions.
- The next three bits contain the encoded DMA channel number (MSB first).
- The next bit (ACT) indicates whether the request for the indicated DMA channel is active or inactive. The ACT bit is 1 (high) to indicate if it is active and 0 (low) if it is inactive. The case where ACT is low is rare, and is only used to indicate that a previous request for that channel is being abandoned.
- After the active/inactive indication, the LDRQ# signal must go high for at least one clock. After that one clock, LDRQ# signal can be brought low to the next encoding sequence.

If another DMA channel also needs to request a transfer, another sequence can be sent on LDRQ#. For example, if an encoded request is sent for Channel 2, and then Channel 3 needs a transfer before the cycle for Channel 2 is run on the interface, the peripheral can send the encoded request for Channel 3. This allows multiple DMA agents behind an I/O device to request use of the LPC interface, and the I/O device does not need to self-arbitrate before sending the message.

Figure 3-4. DMA Request Assertion through LDRQ#



3.6.2 Abandoning DMA Requests

DMA Requests can be de-asserted in two fashions: on error conditions by sending an LDRQ# message with the 'ACT' bit cleared to 0, or normally through a SYNC field during the DMA transfer. This section describes boundary conditions where the DMA request needs to be removed prior to a data transfer.

There may be some special cases where the peripheral desires to abandon a DMA transfer. The most likely case of this occurring is due to a floppy disk controller which has overrun or underrun its FIFO, or software stopping a device prematurely.

In these cases, the peripheral wishes to stop further DMA activity. It may do so by sending an LDRQ# message with the ACT bit as 0. However, since the DMA request was seen by Intel® Xeon® Processor D-1500 Product Family, there is no assurance that the cycle has not been granted and will shortly run on LPC. Therefore, peripherals must take into account that a DMA cycle may still occur. The peripheral can choose not to respond to this cycle, in which case the host will abort it, or it can choose to complete the cycle normally with any random data.

This method of DMA de-assertion should be prevented whenever possible, to limit boundary conditions both on Intel® Xeon® Processor D-1500 Product Family and the peripheral.

3.6.3 General Flow of DMA Transfers

Arbitration for DMA channels is performed through the 8237 within the host. Once the host has won arbitration on behalf of a DMA channel assigned to LPC, it asserts LFRAME# on the LPC I/F and begins the DMA transfer. The general flow for a basic DMA transfer is as follows:

1. Intel® Xeon® Processor D-1500 Product Family starts transfer by asserting 0000b on LAD[3:0] with LFRAME# asserted.
2. Intel® Xeon® Processor D-1500 Product Family asserts 'cycle type' of DMA, direction based on DMA transfer direction.
3. Intel® Xeon® Processor D-1500 Product Family asserts channel number and, if applicable, terminal count.
4. Intel® Xeon® Processor D-1500 Product Family indicates the size of the transfer: 8 or 16 bits.
5. If a DMA reads…
   — Intel® Xeon® Processor D-1500 Product Family drives the first 8 bits of data and turns the bus around.

- The peripheral acknowledges the data with a valid SYNC.
- If a 16-bit transfer, the process is repeated for the next 8 bits.

6. If a DMA writes…
   - Intel® Xeon® Processor D-1500 Product Family turns the bus around and waits for data.
   - The peripheral indicates data ready through SYNC and transfers the first byte.
   - If a 16-bit transfer, the peripheral indicates data ready and transfers the next byte.
7. The peripheral turns around the bus.

3.6.4 Terminal Count

Terminal count is communicated through LAD[3] on the same clock that DMA channel is communicated on LAD[2:0]. This field is the CHANNEL field. Terminal count indicates the last byte of transfer, based upon the size of the transfer.

For example, on an 8-bit transfer size (SIZE field is 00b), if the TC bit is set, then this is the last byte. On a 16-bit transfer (SIZE field is 01b), if the TC bit is set, then the second byte is the last byte. The peripheral, therefore, must internalize the TC bit when the CHANNEL field is communicated, and only signal TC when the last byte of that transfer size has been transferred.

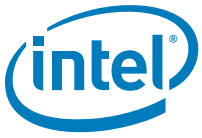
3.6.5 Verify Mode

Verify mode is supported on the LPC interface. A verify transfer to the peripheral is similar to a DMA write, where the peripheral is transferring data to main memory. The indication from the host is the same as a DMA write, so the peripheral will be driving data onto the LPC interface. However, the host will not transfer this data into main memory.

3.6.6 DMA Request De-assertion

An end of transfer is communicated to Intel® Xeon® Processor D-1500 Product Family through a special SYNC field transmitted by the peripheral. An LPC device must not attempt to signal the end of a transfer by de-asserting LDREQ#. If a DMA transfer is several bytes (such as, a transfer from a demand mode device) Intel® Xeon® Processor D-1500 Product Family needs to know when to de-assert the DMA request based on the data currently being transferred.

The DMA agent uses a SYNC encoding on each byte of data being transferred, which indicates to Intel® Xeon® Processor D-1500 Product Family whether this is the last byte of transfer or if more bytes are requested. To indicate the last byte of transfer, the peripheral uses a SYNC value of 0000b (ready with no error), or 1010b (ready with error). These encodings tell Intel® Xeon® Processor D-1500 Product Family that this is the last piece of data transferred on a DMA read (Intel® Xeon® Processor D-1500 Product Family to peripheral), or the byte that follows is the last piece of data transferred on a DMA write (peripheral to Intel® Xeon® Processor D-1500 Product Family).



When Intel® Xeon® Processor D-1500 Product Family sees one of these two encodings, it ends the DMA transfer after this byte and de-asserts the DMA request to the 8237. Therefore, if Intel® Xeon® Processor D-1500 Product Family indicated a 16-bit transfer, the peripheral can end the transfer after one byte by indicating a SYNC value of 0000b or 1010b. Intel® Xeon® Processor D-1500 Product Family does not attempt to transfer the second byte, and de-asserts the DMA request internally.

If the peripheral indicates a 0000b or 1010b SYNC pattern on the last byte of the indicated size, then Intel® Xeon® Processor D-1500 Product Family only de-asserts the DMA request to the 8237 since it does not need to end the transfer.

If the peripheral wishes to keep the DMA request active, then it uses a SYNC value of 1001b (ready plus more data). This tells the 8237 that more data bytes are requested after the current byte has been transferred, so Intel® Xeon® Processor D-1500 Product Family keeps the DMA request active to the 8237. Therefore, on an 8-bit transfer size, if the peripheral indicates a SYNC value of 1001b to Intel® Xeon® Processor D-1500 Product Family, the data will be transferred and the DMA request will remain active to the 8237. At a later time, Intel® Xeon® Processor D-1500 Product Family will then come back with another START–CYCTYPE–CHANNEL–SIZE and so on combination to initiate another transfer to the peripheral.

The peripheral must not assume that the next START indication from Intel® Xeon® Processor D-1500 Product Family is another grant to the peripheral if it had indicated a SYNC value of 1001b. On a single mode DMA device, the 8237 will re-arbitrate after every transfer. Only demand mode DMA devices can be assured that they will receive the next START indication from Intel® Xeon® Processor D-1500 Product Family.

Note: Indicating a 0000b or 1010b encoding on the SYNC field of an odd byte of a 16-bit channel (first byte of a 16-bit transfer) is an error condition.

Note: The host stops the transfer on the LPC bus as indicated, fills the upper byte with random data on DMA writes (peripheral to memory), and indicates to the 8237 that the DMA transfer occurred, incrementing the 8237's address and decrementing its byte count.

3.6.7 SYNC Field / LDRQ# Rules

Since DMA transfers on LPC are requested through an LDRQ# assertion message, and are ended through a SYNC field during the DMA transfer, the peripheral must obey the following rule when initiating back-to-back transfers from a DMA channel.

The peripheral must not assert another message for eight LCLKs after a de-assertion is indicated through the SYNC field. This is needed to allow the 8237, that typically runs off a much slower internal clock, to see a message de-asserted before it is re-asserted so that it can arbitrate to the next agent.

Under default operation, the host only performs 8-bit transfers on 8-bit channels and 16-bit transfers on 16-bit channels.

The method by which this communication between host and peripheral through system BIOS is performed is beyond the scope of this specification. Since the LPC host and LPC peripheral are motherboard devices, no "plug-n-play" registry is required.

The peripheral must not assume that the host is able to perform transfer sizes that are larger than the size allowed for the DMA channel, and be willing to accept a SIZE field that is smaller than what it may currently have buffered.

To that end, it is recommended that future devices that may appear on the LPC bus, that require higher bandwidth than 8-bit or 16-bit DMA allow, do so with a bus mastering interface and not rely on the 8237.

3.7 8254 Timers (D31:F0)

Intel® Xeon® Processor D-1500 Product Family contains three counters that have fixed uses. All registers and functions associated with the 8254 timers are in the core well. The 8254 unit is clocked by a 14.318-MHz clock.

Counter 0, System Timer

This counter functions as the system timer by controlling the state of IRQ0 and is typically programmed for Mode 3 operation. The counter produces a square wave with a period equal to the product of the counter period (838 ns) and the initial count value. The counter loads the initial count value 1 counter period after software writes the count value to the counter I/O address. The counter initially asserts IRQ0 and decrements the count value by two each counter period. The counter negates IRQ0 when the count value reaches 0. It then reloads the initial count value and again decrements the initial count value by two each counter period. The counter then asserts IRQ0 when the count value reaches 0, reloads the initial count value, and repeats the cycle, alternately asserting and negating IRQ0.

Counter 1, Refresh Request Signal

This counter provides the refresh request signal and is typically programmed for Mode 2 operation and only impacts the period of the REF_TOGGLE bit in Port 61. The initial count value is loaded one counter period after being written to the counter I/O address. The REF_TOGGLE bit will have a square wave behavior (alternate between 0 and 1) and will toggle at a rate based on the value in the counter. Programming the counter to anything other than Mode 2 will result in undefined behavior for the REF_TOGGLE bit.

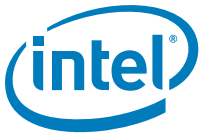
Counter 2, Speaker Tone

This counter provides the speaker tone and is typically programmed for Mode 3 operation. The counter provides a speaker frequency equal to the counter clock frequency (1.193 MHz) divided by the initial count value. The speaker must be enabled by a write to port 061h (see NMI Status and Control ports).

3.7.1 Timer Programming

The counter/timers are programmed in the following fashion:

1. Write a control word to select a counter.
2. Write an initial count for that counter.
3. Load the least and/or most significant bytes (as required by Control Word Bits 5, 4) of the 16-bit counter.
4. Repeat with other counters.



Only two conventions need to be observed when programming the counters. First, for each counter, the control word must be written before the initial count is written. Second, the initial count must follow the count format specified in the control word (least significant byte only, most significant byte only, or least significant byte and then most significant byte).

A new initial count may be written to a counter at any time without affecting the counter's programmed mode. Counting is affected as described in the mode definitions. The new count must follow the programmed count format.

If a counter is programmed to read/write two-byte counts, the following precaution applies: A program must not transfer control between writing the first and second byte to another routine which also writes into that same counter. Otherwise, the counter will be loaded with an incorrect count.

The Control Word Register at port 43h controls the operation of all three counters. Several commands are available:

- **Control Word Command.** Specifies which counter to read or write, the operating mode, and the count format (binary or BCD).
- **Counter Latch Command.** Latches the current count so that it can be read by the system. The countdown process continues.
- **Read Back Command.** Reads the count value, programmed mode, the current state of the OUT pins, and the state of the Null Count Flag of the selected counter.

Table 3-12 lists the six operating modes for the interval counters.

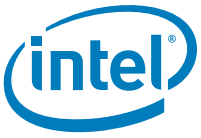
Table 3-12. Counter Operating Modes

Mode	Function	Description
0	Out signal on end of count (=0)	Output is 0. When count goes to 0, output goes to 1 and stays at 1 until counter is reprogrammed.
1	Hardware retriggerable one-shot	Output is 0. When count goes to 0, output goes to 1 for one clock time.
2	Rate generator (divide by n counter)	Output is 1. Output goes to 0 for one clock time, then back to 1 and counter is reloaded.
3	Square wave output	Output is 1. Output goes to 0 when counter rolls over, and counter is reloaded. Output goes to 1 when counter rolls over, and counter is reloaded, and so on.
4	Software triggered strobe	Output is 1. Output goes to 0 when count expires for one clock time.
5	Hardware triggered strobe	Output is 1. Output goes to 0 when count expires for one clock time.

3.7.2 Reading From the Interval Timer

It is often desirable to read the value of a counter without disturbing the count in progress. There are three methods for reading the counters: a simple read operation, counter Latch command, and the Read-Back command. Each is explained below.

With the simple read and counter latch command methods, the count must be read according to the programmed format; specifically, if the counter is programmed for two byte counts, two bytes must be read. The two bytes do not have to be read one right after the other. Read, write, or programming operations for other counters may be inserted between them.



3.7.2.1 Simple Read

The first method is to perform a simple read operation. The counter is selected through Port 40h (Counter 0), 41h (Counter 1), or 42h (Counter 2).

Note: Performing a direct read from the counter does not return a determinate value, because the counting process is asynchronous to read operations. However, in the case of Counter 2, the count can be stopped by writing to the GATE bit in Port 61h.

3.7.2.2 Counter Latch Command

The Counter Latch command, written to Port 43h, latches the count of a specific counter at the time the command is received. This command is used to ensure that the count read from the counter is accurate, particularly when reading a two-byte count. The count value is then read from each counter's Count register as was programmed by the Control register.

The count is held in the latch until it is read or the counter is reprogrammed. The count is then unlatched. This allows reading the contents of the counters on the fly without affecting counting in progress. Multiple Counter Latch Commands may be used to latch more than one counter. Counter Latch commands do not affect the programmed mode of the counter in any way.

If a Counter is latched and then, some time later, latched again before the count is read, the second Counter Latch command is ignored. The count read is the count at the time the first Counter Latch command was issued.

3.7.2.3 Read Back Command

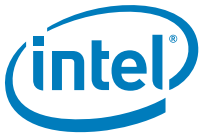
The Read Back command, written to Port 43h, latches the count value, programmed mode, and current states of the OUT pin and Null Count flag of the selected counter or counters. The value of the counter and its status may then be read by I/O access to the counter address.

The Read Back command may be used to latch multiple counter outputs at one time. This single command is functionally equivalent to several counter latch commands, one for each counter latched. Each counter's latched count is held until it is read or reprogrammed. Once read, a counter is unlatched. The other counters remain latched until they are read. If multiple count Read Back commands are issued to the same counter without reading the count, all but the first are ignored.

The Read Back command may additionally be used to latch status information of selected counters. The status of a counter is accessed by a read from that counter's I/O port address. If multiple counter status latch operations are performed without reading the status, all but the first are ignored.

Both count and status of the selected counters may be latched simultaneously. This is functionally the same as issuing two consecutive, separate Read Back commands. If multiple count and/or status Read Back commands are issued to the same counters without any intervening reads, all but the first are ignored.

If both count and status of a counter are latched, the first read operation from that counter returns the latched status, regardless of which was latched first. The next one or two reads, depending on whether the counter is programmed for one or two type counts, returns the latched count. Subsequent reads return unlatched count.



3.8 8259 Programmable Interrupt Controllers (PIC) (D31:F0)

Intel® Xeon® Processor D-1500 Product Family incorporates the functionality of two 8259 interrupt controllers that provide system interrupts for the ISA compatible interrupts. These interrupts can include: system timer, keyboard controller, serial ports, parallel ports, floppy disk, mouse, and DMA channels. In addition, this interrupt controller can support the PCI based interrupts, by mapping the PCI interrupt onto the compatible ISA interrupt line. Each 8259 controller supports eight interrupts, numbered 0–7. Table 3-13 shows how the controllers are connected.

Table 3-13. Interrupt Controller Connections

8259	8259 Input	Typical Interrupt Source	Connected Pin / Function
Master	0	Internal	Internal Timer / Counter 0 output / HPET #0
	1	Keyboard	IRQ1 using SERIRQ
	2	Internal	Slave controller INTR output
	3	Serial Port A	IRQ3 using SERIRQ,
	4	Serial Port B	IRQ4 using SERIRQ, PIRQ#
	5	Parallel Port / Generic	IRQ5 using SERIRQ, PIRQ#
	6	Floppy Disk	IRQ6 using SERIRQ, PIRQ#
	7	Parallel Port / Generic	IRQ7 using SERIRQ, PIRQ#
Slave	0	Internal Real Time Clock	Internal RTC / HPET #1
	1	Generic	IRQ9 using SERIRQ, SCI, TCO, or PIRQ#
	2	Generic	IRQ10 using SERIRQ, SCI, TCO, or PIRQ#
	3	Generic	IRQ11 using SERIRQ, SCI, TCO, or PIRQ#, or HPET #2
	4	PS/2 Mouse	IRQ12 using SERIRQ, SCI, TCO, or PIRQ#, or HPET #3
	5	Internal	State Machine output based on processor FERR# assertion. May optionally be used for SCI or TCO interrupt if FERR# not needed.
	6	SATA	SATA Primary (legacy mode), or using SERIRQ or PIRQ#
	7	SATA	SATA Secondary (legacy mode) or using SERIRQ or PIRQ#

Intel® Xeon® Processor D-1500 Product Family cascades the slave controller onto the master controller through master controller interrupt input 2. This means there are only 15 possible interrupts for Intel® Xeon® Processor D-1500 Product Family PIC.

Interrupts can individually be programmed to be edge or level, except for IRQ0, IRQ2, IRQ8#, and IRQ13.

Note: Active-low interrupt sources (such as, the PIRQ#s) are inverted inside Intel® Xeon® Processor D-1500 Product Family. In the following descriptions of the 8259s, the interrupt levels are in reference to the signals at the internal interface of the 8259s, after the required inversions have occurred. Therefore, the term “high” indicates “active,” which means “low” on an originating PIRQ#.

3.8.1 Interrupt Handling

3.8.1.1 Generating Interrupts

The PIC interrupt sequence involves three bits, from the IRR, ISR, and IMR, for each interrupt level. These bits are used to determine the interrupt vector returned, and status of any other pending interrupts. Table 3-14 defines the IRR, ISR, and IMR.

Table 3-14. Interrupt Status Registers

Bit	Description
IRR	**Interrupt Request Register.** This bit is set on a low to high transition of the interrupt line in edge mode, and by an active high level in level mode. This bit is set whether or not the interrupt is masked. However, a masked interrupt will not generate INTR.
ISR	**Interrupt Service Register.** This bit is set, and the corresponding IRR bit cleared, when an interrupt acknowledge cycle is seen, and the vector returned is for that interrupt.
IMR	**Interrupt Mask Register.** This bit determines whether an interrupt is masked. Masked interrupts will not generate INTR.

3.8.1.2 Acknowledging Interrupts

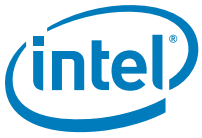
The processor generates an interrupt acknowledge cycle that is translated by the host bridge into a PCI Interrupt Acknowledge Cycle to Intel® Xeon® Processor D-1500 Product Family. The PIC translates this command into two internal INTA# pulses expected by the 8259 cores. The PIC uses the first internal INTA# pulse to freeze the state of the interrupts for priority resolution. On the second INTA# pulse, the master or slave sends the interrupt vector to the processor with the acknowledged interrupt code. This code is based upon Bits 7:3 of the corresponding ICW2 register, combined with three bits representing the interrupt within that controller.

Table 3-15. Content of Interrupt Vector Byte

Master, Slave Interrupt	Bits [7:3]	Bits [2:0]
IRQ7,15	ICW2[7:3]	111
IRQ6,14		110
IRQ5,13		101
IRQ4,12		100
IRQ3,11		011
IRQ2,10		010
IRQ1,9		001
IRQ0,8		000

3.8.1.3 Hardware/Software Interrupt Sequence

1. One or more of the Interrupt Request lines (IRQ) are raised high in edge mode, or seen high in level mode, setting the corresponding IRR bit.
2. The PIC sends INTR active to the processor if an asserted interrupt is not masked.
3. The processor acknowledges the INTR and responds with an interrupt acknowledge cycle. The cycle is translated into a PCI interrupt acknowledge cycle by the host bridge. This command is broadcast over PCI by Intel® Xeon® Processor D-1500 Product Family.
4. Upon observing its own interrupt acknowledge cycle on PCI, Intel® Xeon® Processor D-1500 Product Family converts it into the two cycles that the internal 8259 pair can respond to. Each cycle appears as an interrupt acknowledge pulse on the internal INTA# pin of the cascaded interrupt controllers.



5. Upon receiving the first internally generated INTA# pulse, the highest priority ISR bit is set and the corresponding IRR bit is reset. On the trailing edge of the first pulse, a slave identification code is broadcast by the master to the slave on a private, internal three bit wide bus. The slave controller uses these bits to determine if it must respond with an interrupt vector during the second INTA# pulse.
6. Upon receiving the second internally generated INTA# pulse, the PIC returns the interrupt vector. If no interrupt request is present because the request was too short in duration, the PIC returns vector 7 from the master controller.
7. This completes the interrupt cycle. In AEOI mode the ISR bit is reset at the end of the second INTA# pulse. Otherwise, the ISR bit remains set until an appropriate EOI command is issued at the end of the interrupt subroutine.

3.8.2 Initialization Command Words (ICWx)

Before operation can begin, each 8259 must be initialized. In Intel® Xeon® Processor D-1500 Product Family, this is a four byte sequence. The four initialization command words are referred to by their acronyms: ICW1, ICW2, ICW3, and ICW4.

The base address for each 8259 initialization command word is a fixed location in the I/O memory space: 20h for the master controller, and A0h for the slave controller.

3.8.2.1 ICW1

An I/O write to the master or slave controller base address with data bit 4 equal to 1 is interpreted as a write to ICW1. Upon sensing this write, Intel® Xeon® Processor D-1500 Product Family's PIC expects three more byte writes to 21h for the master controller, or A1h for the slave controller, to complete the ICW sequence.

A write to ICW1 starts the initialization sequence during which the following automatically occur:

1. Following initialization, an interrupt request (IRQ) input must make a low-to-high transition to generate an interrupt.
2. The Interrupt Mask Register is cleared.
3. IRQ7 input is assigned priority 7.
4. The slave mode address is set to 7.
5. Special mask mode is cleared and Status Read is set to IRR.

3.8.2.2 ICW2

The second write in the sequence (ICW2) is programmed to provide bits [7:3] of the interrupt vector that will be released during an interrupt acknowledge. A different base is selected for each interrupt controller.

3.8.2.3 ICW3

The third write in the sequence (ICW3) has a different meaning for each controller.

- For the master controller, ICW3 is used to indicate which IRQ input line is used to cascade the slave controller. Within Intel® Xeon® Processor D-1500 Product Family, IRQ2 is used. Therefore, Bit 2 of ICW3 on the master controller is set to a 1, and the other bits are cleared to 0s.

- For the slave controller, ICW3 is the slave identification code used during an interrupt acknowledge cycle. On interrupt acknowledge cycles, the master controller broadcasts a code to the slave controller if the cascaded interrupt won arbitration on the master controller. The slave controller compares this identification code to the value stored in its ICW3, and if it matches, the slave controller assumes responsibility for broadcasting the interrupt vector.

3.8.2.4 ICW4

The final write in the sequence (ICW4) must be programmed for both controllers. At the very least, Bit 0 must be set to a 1 to indicate that the controllers are operating in an Intel® architecture-based system.

3.8.3 Operation Command Words (OCW)

These command words reprogram the Interrupt controller to operate in various interrupt modes.

- OCW1 masks and unmasks interrupt lines.
- OCW2 controls the rotation of interrupt priorities when in rotating priority mode, and controls the EOI function.
- OCW3 sets up ISR/IRR reads, enables/disables the special mask mode (SMM), and enables/disables polled interrupt mode.

3.8.4 Modes of Operation

3.8.4.1 Fully Nested Mode

In this mode, interrupt requests are ordered in priority from 0 through 7, with 0 being the highest. When an interrupt is acknowledged, the highest priority request is determined and its vector placed on the bus. Additionally, the ISR for the interrupt is set. This ISR bit remains set until: the processor issues an EOI command immediately before returning from the service routine; or if in AEOI mode, on the trailing edge of the second INTA#. While the ISR bit is set, all further interrupts of the same or lower priority are inhibited, while higher levels generate another interrupt. Interrupt priorities can be changed in the rotating priority mode.

3.8.4.2 Special Fully-Nested Mode

This mode is used in the case of a system where cascading is used, and the priority has to be conserved within each slave. In this case, the special fully-nested mode is programmed to the master controller. This mode is similar to the fully-nested mode with the following exceptions:

- When an interrupt request from a certain slave is in service, this slave is not locked out from the master's priority logic and further interrupt requests from higher priority interrupts within the slave are recognized by the master and initiate interrupts to the processor. In the normal-nested mode, a slave is masked out when its request is in service.
- When exiting the Interrupt Service routine, software has to check whether the interrupt serviced was the only one from that slave. This is done by sending a Non-

Specific EOI command to the slave and then reading its ISR. If it is 0, a non-specific EOI can also be sent to the master.

3.8.4.3 Automatic Rotation Mode (Equal Priority Devices)

In some applications, there are a number of interrupting devices of equal priority. Automatic rotation mode provides for a sequential 8-way rotation. In this mode, a device receives the lowest priority after being serviced. In the worst case, a device requesting an interrupt has to wait until each of seven other devices are serviced at most once.

There are two ways to accomplish automatic rotation using OCW2; the Rotation on Non-Specific EOI Command (R=1, SL=0, EOI=1) and the rotate in automatic EOI mode which is set by (R=1, SL=0, EOI=0).

3.8.4.4 Specific Rotation Mode (Specific Priority)

Software can change interrupt priorities by programming the bottom priority. For example, if IRQ5 is programmed as the bottom priority device, then IRQ6 is the highest priority device. The Set Priority Command is issued in OCW2 to accomplish this, where: R=1, SL=1, and LO–L2 is the binary priority level code of the bottom priority device.

In this mode, internal status is updated by software control during OCW2. However, it is independent of the EOI command. Priority changes can be executed during an EOI command by using the Rotate on Specific EOI Command in OCW2 (R=1, SL=1, EOI=1 and LO–L2=IRQ level to receive bottom priority.

3.8.4.5 Poll Mode

Poll mode can be used to conserve space in the interrupt vector table. Multiple interrupts that can be serviced by one interrupt service routine do not need separate vectors if the service routine uses the poll command. Poll mode can also be used to expand the number of interrupts. The polling interrupt service routine can call the appropriate service routine, instead of providing the interrupt vectors in the vector table. In this mode, the INTR output is not used and the microprocessor internal Interrupt Enable flip-flop is reset, disabling its interrupt input. Service to devices is achieved by software using a Poll command.

The Poll command is issued by setting P=1 in OCW3. The PIC treats its next I/O read as an interrupt acknowledge, sets the appropriate ISR bit if there is a request, and reads the priority level. Interrupts are frozen from the OCW3 write to the I/O read. The byte returned during the I/O read contains a 1 in Bit 7 if there is an interrupt, and the binary code of the highest priority level in Bits 2:0.

3.8.4.6 Edge and Level Triggered Mode

In ISA systems this mode is programmed using Bit 3 in ICW1, which sets level or edge for the entire controller. In Intel® Xeon® Processor D-1500 Product Family, this bit is disabled and a register for edge and level triggered mode selection, per interrupt input, is included. This is the Edge/Level control Registers ELCR1 and ELCR2.

If an ELCR bit is 0, an interrupt request will be recognized by a low-to-high transition on the corresponding IRQ input. The IRQ input can remain high without generating another interrupt. If an ELCR bit is 1, an interrupt request will be recognized by a high

level on the corresponding IRQ input and there is no need for an edge detection. The interrupt request must be removed before the EOI command is issued to prevent a second interrupt from occurring.

In both the edge and level triggered modes, the IRQ inputs must remain active until after the falling edge of the first internal INTA#. If the IRQ input goes inactive before this time, a default IRQ7 vector is returned.

3.8.4.7 End of Interrupt (EOI) Operations

An EOI can occur in one of two fashions: by a command word write issued to the PIC before returning from a service routine, the EOI command; or automatically when AEOI bit in ICW4 is set to 1.

3.8.4.8 Normal End of Interrupt

In normal EOI, software writes an EOI command before leaving the interrupt service routine to mark the interrupt as completed. There are two forms of EOI commands: Specific and Non-Specific. When a Non-Specific EOI command is issued, the PIC clears the highest ISR bit of those that are set to 1. Non-Specific EOI is the normal mode of operation of the PIC within Intel® Xeon® Processor D-1500 Product Family, as the interrupt being serviced currently is the interrupt entered with the interrupt acknowledge. When the PIC is operated in modes that preserve the fully nested structure, software can determine which ISR bit to clear by issuing a Specific EOI. An ISR bit that is masked is not cleared by a Non-Specific EOI if the PIC is in the special mask mode. An EOI command must be issued for both the master and slave controller.

3.8.4.9 Automatic End of Interrupt Mode

In this mode, the PIC automatically performs a Non-Specific EOI operation at the trailing edge of the last interrupt acknowledge pulse. From a system standpoint, this mode should be used only when a nested multi-level interrupt structure is not required within a single PIC. The AEOI mode can only be used in the master controller and not the slave controller.

3.8.5 Masking Interrupts

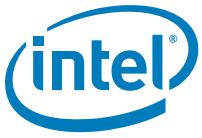
3.8.5.1 Masking on an Individual Interrupt Request

Each interrupt request can be masked individually by the Interrupt Mask Register (IMR). This register is programmed through OCW1. Each bit in the IMR masks one interrupt channel. Masking IRQ2 on the master controller masks all requests for service from the slave controller.

3.8.5.2 Special Mask Mode

Some applications may require an interrupt service routine to dynamically alter the system priority structure during its execution under software control. For example, the routine may wish to inhibit lower priority requests for a portion of its execution but enable some of them for another portion.

The special mask mode enables all interrupts not masked by a bit set in the Mask register. Normally, when an interrupt service routine acknowledges an interrupt without issuing an EOI to clear the ISR bit, the interrupt controller inhibits all lower priority



requests. In the special mask mode, any interrupts may be selectively enabled by loading the Mask Register with the appropriate pattern. The special mask mode is set by OCW3 where: SSMM=1, SMM=1, and cleared where SSMM=1, SMM=0.

3.8.6 Steering PCI Interrupts

Intel® Xeon® Processor D-1500 Product Family can be programmed to allow PIRQA#-PIRQH# to be routed internally to interrupts 3–7, 9–12, 14 or 15. The assignment is programmable through the PIRQx Route Control registers, located at 60–63h and 68–6Bh in D31:F0. One or more PIRQx# lines can be routed to the same IRQx input. If interrupt steering is not required, the Route registers can be programmed to disable steering.

The PIRQx# lines are defined as active low, level sensitive to allow multiple interrupts on a PCI board to share a single line across the connector. When a PIRQx# is routed to specified IRQ line, software must change the IRQ's corresponding ELCR bit to level sensitive mode. Intel® Xeon® Processor D-1500 Product Family internally inverts the PIRQx# line to send an active high level to the PIC. When a PCI interrupt is routed onto the PIC, the selected IRQ can no longer be used by an active high device (through SERIRQ). However, active low interrupts can share their interrupt with PCI interrupts.

Internal sources of the PIRQs, including SCI and TCO interrupts, cause the external PIRQ to be asserted. Intel® Xeon® Processor D-1500 Product Family receives the PIRQ input, like all of the other external sources, and routes it accordingly.

3.9 Advanced Programmable Interrupt Controller (APIC) (D31:F0)

In addition to the standard ISA-compatible PIC described in the previous section, Intel® Xeon® Processor D-1500 Product Family incorporates the APIC. While the standard interrupt controller is intended for use in a uni-processor system, APIC can be used in either a uni-processor or multi-processor system.

3.9.1 Interrupt Handling

The I/O APIC handles interrupts very differently than the 8259. Briefly, these differences are:

- Method of Interrupt Transmission. The I/O APIC transmits interrupts through memory writes on the normal data path to the processor, and interrupts are handled without the need for the processor to run an interrupt acknowledge cycle.
- **Interrupt Priority.** The priority of interrupts in the I/O APIC is independent of the interrupt number. For example, interrupt 10 can be given a higher priority than interrupt 3.
- **More Interrupts.** The I/O APIC in Intel® Xeon® Processor D-1500 Product Family supports a total of 24 interrupts.
- **Multiple Interrupt Controllers.** The I/O APIC architecture allows for multiple I/O APIC devices in the system with their own interrupt vectors.

3.9.2 Interrupt Mapping

The I/O APIC within Intel® Xeon® Processor D-1500 Product Family supports 24 APIC interrupts. Each interrupt has its own unique vector assigned by software. The interrupt vectors are mapped as shown in the following table:

Table 3-16. APIC Interrupt Mapping[1]

IRQ #	Using SERIRQ	Direct from Pin	Using PCI Message	Internal Modules
0	No	No	No	Cascade from 8259 #1
1	Yes	No	Yes	
2	No	No	No	8254 Counter 0, HPET #0 (legacy mode)
3	Yes	No	Yes	
4	Yes	No	Yes	
5	Yes	No	Yes	
6	Yes	No	Yes	
7	Yes	No	Yes	
8	No	No	No	RTC, HPET #1 (legacy mode)
9	Yes	No	Yes	Option for SCI, TCO
10	Yes	No	Yes	Option for SCI, TCO
11	Yes	No	Yes	HPET #2, Option for SCI, TCO (Note 2)
12	Yes	No	Yes	HPET #3 (Note 3)
13	No	No	No	FERR# logic
14	Yes	No	Yes	SATA Primary (legacy mode)
15	Yes	No	Yes	SATA Secondary (legacy mode)
16	PIRQA#	PIRQA#	Yes	Internal devices are routable; see Section 5.1.16 though Section 5.1.32.
17	PIRQB#	PIRQB#		
18	PIRQC#	PIRQC#		
19	PIRQD#	PIRQD#		
20	N/A	PIRQE#4	Yes	Option for SCI, TCO, HPET #0,1,2, 3. Other internal devices are routable; see Section 5.1.16 though Section 5.1.32.
21	N/A	PIRQF#4		
22	N/A	PIRQG#4		
23	N/A	PIRQH#4		

Notes:
1. When programming the polarity of internal interrupt sources on the APIC, interrupts 0 through 15 receive active-high internal interrupt sources, while interrupts 16 through 23 receive active-low internal interrupt sources.
2. If IRQ 11 is used for HPET #2, software should ensure IRQ 11 is not shared with any other devices to ensure the proper operation of HPET #2. Intel® Xeon® Processor D-1500 Product Family hardware does not prevent sharing of IRQ 11.
3. If IRQ 12 is used for HPET #3, software should ensure IRQ 12 is not shared with any other devices to ensure the proper operation of HPET #3. Intel® Xeon® Processor D-1500 Product Family hardware does not prevent sharing of IRQ 12.
4. PIRQ[E:H] are Multiplexed with GPIO pins. Interrupts PIRQ[E:H] will not be exposed if they are configured as GPIOs.

3.9.3 PCI / PCI Express* Message-Based Interrupts

When external devices through PCI/PCI Express wish to generate an interrupt, they will send the message defined in the *PCI Express* Base Specification,* Revision 2.0 for generating INTA# – INTD#. These will be translated internal assertions/de-assertions of INTA# – INTD#.

3.9.4 IOxAPIC Address Remapping

To support Intel Virtualization Technology, interrupt messages are required to go through similar address remapping as any other memory request. Address remapping allows for domain isolation for interrupts, so a device assigned in one domain is not allowed to generate an interrupt to another domain.

The address remapping is based on the Bus: Device: Function field associated with the requests. The internal APIC is required to initiate the interrupt message using a unique Bus: Device: Function.

Intel® Xeon® Processor D-1500 Product Family allows BIOS to program the unique Bus: Device: Function address for the internal APIC. This address field does not change the APIC functionality and the APIC is not promoted as a stand-alone PCI device. See Device 31: Function 0 Offset 6Ch for additional information.

3.9.5 External Interrupt Controller Support

Intel® Xeon® Processor D-1500 Product Family supports external APICs off of PCI Express ports but does not support APICs on the PCI bus. The EOI special cycle is only forwarded to PCI Express ports.

3.10 Serial Interrupt (D31:F0)

Intel® Xeon® Processor D-1500 Product Family supports a serial IRQ scheme. This allows a single signal to be used to report interrupt requests. The signal used to transmit this information is shared between Intel® Xeon® Processor D-1500 Product Family and all participating peripherals. The signal line, SERIRQ, is synchronous to PCI clock, and follows the sustained tri-state protocol that is used by all PCI signals. This means that if a device has driven SERIRQ low, it will first drive it high synchronous to PCI clock and release it the following PCI clock. The serial IRQ protocol defines this sustained tri-state signaling in the following fashion:

- **S – Sample Phase.** Signal driven low
- **R** – **Recovery Phase.** Signal driven high
- **T** – **Turn-around Phase.** Signal released

Intel® Xeon® Processor D-1500 Product Family supports a message for 21 serial interrupts. These represent the 15 ISA interrupts (IRQ0–1, 3–15), the four PCI interrupts, and the control signals SMI# and IOCHK#. The serial IRQ protocol does not support the additional APIC interrupts (20–23).

Note: When the SATA controller is configured for legacy IDE mode, IRQ14 and IRQ15 are expected to behave as ISA legacy interrupts that cannot be shared (that is, through the Serial Interrupt pin). If IRQ14 and IRQ15 are shared with Serial Interrupt pin then

abnormal system behavior may occur. For example, IRQ14/15 may not be detected by Intel® Xeon® Processor D-1500 Product Family's interrupt controller. When the SATA controller is not running in Native IDE mode, IRQ14 and IRQ15 are used as special interrupts. If the SATA controller is in native mode, these interrupts can be mapped to other devices accordingly.

3.10.1 Start Frame

The serial IRQ protocol has two modes of operation which affect the start frame. These two modes are: Continuous, where Intel® Xeon® Processor D-1500 Product Family is solely responsible for generating the start frame; and Quiet, where a serial IRQ peripheral is responsible for beginning the start frame.

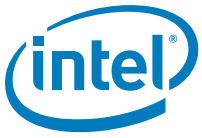
The mode that must first be entered when enabling the serial IRQ protocol is continuous mode. In this mode, Intel® Xeon® Processor D-1500 Product Family asserts the start frame. This start frame is 4, 6, or 8 PCI clocks wide based upon the Serial IRQ Control Register, bits 1:0 at 64h in D31:F0 configuration space. This is a polling mode.

When the serial IRQ stream enters quiet mode (signaled in the Stop Frame), the SERIRQ line remains inactive and pulled up between the Stop and Start Frame until a peripheral drives the SERIRQ signal low. Intel® Xeon® Processor D-1500 Product Family senses the line low and continues to drive it low for the remainder of the Start Frame. Since the first PCI clock of the start frame was driven by the peripheral in this mode, Intel® Xeon® Processor D-1500 Product Family drives the SERIRQ line low for 1 PCI clock less than in continuous mode. This mode of operation allows for a quiet, and therefore lower power, operation.

3.10.2 Data Frames

Once the Start frame has been initiated, all of the SERIRQ peripherals must start counting frames based on the rising edge of SERIRQ. Each of the IRQ/DATA frames has exactly 3 phases of 1 clock each:

- **Sample Phase.** During this phase, the SERIRQ device drives SERIRQ low if the corresponding interrupt signal is low. If the corresponding interrupt is high, then the SERIRQ devices tri-state the SERIRQ signal. The SERIRQ line remains high due to pull-up resistors (there is no internal pull-up resistor on this signal, an external pull-up resistor is required). A low level during the IRQ0–1 and IRQ2–15 frames indicates that an active-high ISA interrupt is not being requested, but a low level during the PCI INT[A:D], SMI#, and IOCHK# frame indicates that an active-low interrupt is being requested.
- **Recovery Phase.** During this phase, the device drives the SERIRQ line high if in the Sample Phase it was driven low. If it was not driven in the sample phase, it is tri-stated in this phase.
- **Turn-around Phase.** The device tri-states the SERIRQ line



3.10.3 Stop Frame

After all data frames, a Stop Frame is driven by Intel® Xeon® Processor D-1500 Product Family. The SERIRQ signal is driven low by Intel® Xeon® Processor D-1500 Product Family for 2 or 3 PCI clocks. The number of clocks is determined by the SERIRQ configuration register. The number of clocks determines the next mode.

Table 3-17. Stop Frame Explanation

Stop Frame Width	Next Mode
2 PCI clocks	**Quiet Mode.** Any SERIRQ device may initiate a Start Frame
3 PCI clocks	**Continuous Mode.** Only the host (Intel® Xeon® Processor D-1500 Product Family) may initiate a Start Frame

3.10.4 Specific Interrupts Not Supported Using SERIRQ

There are three interrupts seen through the serial stream that are not supported by Intel® Xeon® Processor D-1500 Product Family. These interrupts are generated internally, and are not sharable with other devices within the system. These interrupts are:

- IRQ0. Heartbeat interrupt generated off of the internal 8254 counter 0.
- IRQ8#. RTC interrupt can only be generated internally.
- IRQ13. Floating point error interrupt generated off of the processor assertion of FERR#.

Intel® Xeon® Processor D-1500 Product Family ignores the state of these interrupts in the serial stream, and does not adjust their level based on the level seen in the serial stream.

3.10.5 Data Frame Format

Table 3-18 shows the format of the data frames. For the PCI interrupts (A–D), the output from Intel® Xeon® Processor D-1500 Product Family is AND'd with the PCI input signal. This way, the interrupt can be signaled using both the PCI interrupt input signal and using the SERIRQ signal (they are shared).

Table 3-18. Data Frame Format (Sheet 1 of 2)

Data Frame #	Interrupt	Clocks Past Start Frame	Comment
1	IRQ0	2	Ignored. IRQ0 can only be generated using the internal 8524
2	IRQ1	5	
3	SMI#	8	Causes SMI# if low. Will set the SERIRQ_SMI_STS bit.
4	IRQ3	11	
5	IRQ4	14	
6	IRQ5	17	
7	IRQ6	20	
8	IRQ7	23	
9	IRQ8	26	Ignored. IRQ8# can only be generated internally.
10	IRQ9	29	
11	IRQ10	32	

Table 3-18. Data Frame Format (Sheet 2 of 2)

Data Frame #	Interrupt	Clocks Past Start Frame	Comment
12	IRQ11	35	
13	IRQ12	38	
14	IRQ13	41	Ignored. IRQ13 can only be generated from FERR#
15	IRQ14	44	Not attached to SATA logic
16	IRQ15	47	Not attached to SATA logic
17	IOCHCK#	50	Same as ISA IOCHCK# going active.
18	PCI INTA#	53	Drive PIRQA#
19	PCI INTB#	56	Drive PIRQB#
20	PCI INTC#	59	Drive PIRQC#
21	PCI INTD#	62	Drive PIRQD#

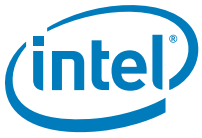
3.11 Real Time Clock (D31:F0)

The Real Time Clock (RTC) module provides a battery backed-up date and time keeping device with two banks of static RAM with 128 bytes each, although the first bank has 114 bytes for general purpose usage. Three interrupt features are available: time of day alarm with once a second to once a month range, periodic rates of 122 µs to 500 ms, and end of update cycle notification. Seconds, minutes, hours, days, day of week, month, and year are counted. Daylight savings compensation is no longer supported. The hour is represented in twelve or twenty-four hour format, and data can be represented in BCD or binary format. The design is functionally compatible with the Motorola MS146818B. The time keeping comes from a 32.768 kHz oscillating source, which is divided to achieve an update every second. The lower 14 bytes on the lower RAM block has very specific functions. The first ten are for time and date information. The next four (0Ah to 0Dh) are registers, which configure and report RTC functions.

The time and calendar data should match the data mode (BCD or binary) and hour mode (12 or 24 hour) as selected in register B. It is up to the programmer to make sure that data stored in these locations is within the reasonable values ranges and represents a possible date and time. The exception to these ranges is to store a value of C0–FFh in the Alarm bytes to indicate a don't care situation. All Alarm conditions must match to trigger an Alarm Flag, which could trigger an Alarm Interrupt if enabled. The SET bit must be 1 while programming these locations to avoid clashes with an update cycle. Access to time and date information is done through the RAM locations. If a RAM read from the ten time and date bytes is attempted during an update cycle, the value read do not necessarily represent the true contents of those locations. Any RAM writes under the same conditions are ignored.

Note: The leap year determination for adding a 29th day to February does not take into account the end-of-the-century exceptions. The logic simply assumes that all years divisible by 4 are leap years. According to the Royal Observatory Greenwich, years that are divisible by 100 are typically not leap years. In every fourth century (years divisible by 400, like 2000), the 100-year-exception is over-ridden and a leap-year occurs. The year 2100 will be the first time in which the current RTC implementation would incorrectly calculate the leap-year.

Intel® Xeon® Processor D-1500 Product Family does not implement month/year alarms.



3.11.1 Update Cycles

An update cycle occurs once a second, if the SET bit of register B is not asserted and the divide chain is properly configured. During this procedure, the stored time and date are incremented, overflow is checked, a matching alarm condition is checked, and the time and date are rewritten to the RAM locations. The update cycle will start at least 488 µs after the UIP bit of register A is asserted, and the entire cycle does not take more than 1984 µs to complete. The time and date RAM locations (0–9) are disconnected from the external bus during this time.

To avoid update and data corruption conditions, external RAM access to these locations can safely occur at two times. When a updated-ended interrupt is detected, almost 999 ms is available to read and write the valid time and date data. If the UIP bit of Register A is detected to be low, there is at least 488 µs before the update cycle begins.

Warning: The overflow conditions for leap years adjustments are based on more than one date or time item. To ensure proper operation when adjusting the time, the new time and data values should be set at least two seconds before leap year occurs.

3.11.2 Interrupts

The real-time clock interrupt is internally routed within Intel® Xeon® Processor D-1500 Product Family both to the I/O APIC and the 8259. It is mapped to interrupt vector 8. This interrupt does not leave Intel® Xeon® Processor D-1500 Product Family, nor is it shared with any other interrupt. IRQ8# from the SERIRQ stream is ignored. However, the High Performance Event Timers can also be mapped to IRQ8#; in this case, the RTC interrupt is blocked.

3.11.3 Lockable RAM Ranges

The RTC battery-backed RAM supports two 8-byte ranges that can be locked using the configuration space. If the locking bits are set, the corresponding range in the RAM will not be readable or writable. A write cycle to those locations will have no effect. A read cycle to those locations will not return the location’s actual value (resultant value is undefined).

Once a range is locked, the range can be unlocked only by a hard reset, which will invoke the BIOS and allow it to relock the RAM range.

3.11.4 Century Rollover

Intel® Xeon® Processor D-1500 Product Family detects a rollover when the Year byte (RTC I/O space, index Offset 09h) transitions form 99 to 00. Upon detecting the rollover, Intel® Xeon® Processor D-1500 Product Family sets the NEWCENTURY_STS bit (TCOBASE + 04h, Bit 7). If the system is in an S0 state, this causes an SMI#. The SMI# handler can update registers in the RTC RAM that are associated with century value. If the system is in a sleep state (S1–S5) when the century rollover occurs, Intel® Xeon® Processor D-1500 Product Family also sets the NEWCENTURY_STS bit, but no SMI# is generated. When the system resumes from the sleep state, BIOS should check the NEWCENTURY_STS bit and update the century value in the RTC RAM.

3.11.5 Clearing Battery-Backed RTC RAM

Clearing CMOS RAM in a Intel® Xeon® Processor D-1500 Product Family-based platform can be done by using a jumper on RTCRST# or GPI. Implementations should not attempt to clear CMOS by using a jumper to pull VccRTC low.

Using RTCRST# to Clear CMOS

A jumper on RTCRST# can be used to clear CMOS values, as well as reset to default, the state of those configuration bits that reside in the RTC power well. When the RTCRST# is strapped to ground, the RTC_PWR_STS bit (D31:F0:A4h Bit 2) will be set and those configuration bits in the RTC power well will be set to their default state. BIOS can monitor the state of this Bit, and manually clear the RTC CMOS array once the system is booted.
The normal position would cause RTCRST# to be pulled up through a weak pull-up resistor. Table 3-19 shows which bits are set to their default state when RTCRST# is asserted. This RTCRST# jumper technique allows the jumper to be moved and then replaced—all while
the system is powered off. Then, once booted, the RTC_PWR_STS can be detected in the
set state.

Table 3-19. Configuration Bits Reset by RTCRST# Assertion (Sheet 1 of 2)

Bit Name	Register	Location	Bit(s)	Default State
Alarm Interrupt Enable (AIE)	Register B (General Configuration) (RTC_REGB)	I/O space (RTC Index + 0Bh)	5	X
Alarm Flag (AF)	Register C (Flag Register) (RTC_REGC)	I/O space (RTC Index + 0Ch)	5	X
SWSMI_RATE_SEL	General PM Configuration 3 Register GEN_PMCON_3	D31:F0:A4h	7:6	0
SLP_S4# Minimum Assertion Width	General PM Configuration 3 Register GEN_PMCON_3	D31:F0:A4h	5:4	0
SLP_S4# Assertion Stretch Enable	General PM Configuration 3 Register GEN_PMCON_3	D31:F0:A4h	3	0
RTC Power Status (RTC_PWR_STS)	General PM Configuration 3 Register GEN_PMCON_3	D31:F0:A4h	2	0
Power Failure (PWR_FLR)	General PM Configuration 3 Register (GEN_PMCON_3)	D31:F0:A4h	1	0
AFTERG3_EN	General PM Configuration 3 Register GEN_PMCON_3	D31:F0:A4h	0	0
Power Button Override Status (PRBTNOR_STS)	Power Management 1 Status Register (PM1_STS)	PMBase + 00h	11	0
RTC Event Enable (RTC_EN)	Power Management 1 Enable Register (PM1_EN)	PMBase + 02h	10	0
Sleep Type (SLP_TYP)	Power Management 1 Control (PM1_CNT)	PMBase + 04h	12:10	0
PME_EN	General Purpose Event 0 Enables Register (GPE0_EN)	PMBase + 2Ch	11	0
RI_EN	General Purpose Event 0 Enables Register (GPE0_EN)	PMBase + 2Ch	8	0

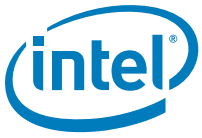


Table 3-19. Configuration Bits Reset by RTCRST# Assertion (Sheet 2 of 2)

Bit Name	Register	Location	Bit(s)	Default State
NEWCENTURY_STS	TCO1 Status Register (TCO1_STS)	TCOBase + 04h	7	0
Intruder Detect (INTRD_DET)	TCO2 Status Register (TCO2_STS)	TCOBase + 06h	0	0
Top Swap (TS)	Backed Up Control Register (BUC)	Chipset Config Registers:Offset 3414h	0	X

Using a GPI to Clear CMOS

A jumper on a GPI can also be used to clear CMOS values. BIOS would detect the setting of this GPI on system boot-up, and manually clear the CMOS array.

Note: The GPI strap technique to clear CMOS requires multiple steps to implement. The system is booted with the jumper in new position, then powered back down. The jumper is replaced back to the normal position, then the system is rebooted again.

Warning: Do not implement a jumper on VccRTC to clear CMOS.

3.12 Power Management

3.12.1 Features

- Support for *Advanced Configuration and Power Interface, Version 4.0a (ACPI)* providing power and thermal management
  - — ACPI 24-Bit Timer SCI and SMI# Generation
- PCI PME# signal for Wake Up from Low-Power states
- System Sleep State Control
  - — ACPI S4 state – Suspend-to-Disk (STD)
  - — ACPI G2/S5 state – Soft Off (SOFF)
  - — Power Failure Detection and Recovery
- Intel® Management Engine (Intel® ME) Power Management Support
  - — Wake events from the Intel® Management Engine (enabled from all S-States including Catastrophic S5 conditions)

3.12.2 Intel® Xeon® Processor D-1500 Product Family and System Power States

Table 3-20 shows the power states defined for Intel® Xeon® Processor D-1500 Product Family-based platforms. The state names generally match the corresponding ACPI states.

Table 3-20. General Power States for Systems Using Intel® Xeon® Processor D-1500 Product Family

State/ Substates	Legacy Name / Description
G0/S0/C0	**Full On:** Processor operating. Individual devices may be shut down or be placed into lower power states to save power.
G0/S0/Cx	**Cx State:** Cx states are processor power states within the S0 system state that provide for various levels of power savings. The processor initiates C-state entry and exit while interacting with Intel® Xeon® Processor D-1500 Product Family. Intel® Xeon® Processor D-1500 Product Family will base its behavior on the processor state.
G1/S1	**S1:** Intel® Xeon® Processor D-1500 Product Family provides the S1 messages and the S0 messages on a wake event. It is preferred for systems to use C-states than S1.
G1/S3	**Suspend-To-RAM (STR):** The system context is maintained in system DRAM, but power is shut off to non-critical circuits. Memory is retained and refreshes continue. All external clocks stop except RTC.
G1/S4	**Suspend-To-Disk (STD):** The context of the system is maintained on the disk. All power is then shut off to the system except for the logic required to resume.
G2/S5	**Soft Off (SOFF):** System context is not maintained. All power is shut off except for the logic required to restart. A full boot is required when waking.
G3	**Mechanical OFF (MOFF):** System context not maintained. All power is shut off except for the RTC. No "Wake" events are possible. This state occurs if the user removes the main system batteries, turns off a mechanical switch, or if the system power supply is at a level that is insufficient to power the "waking" logic. When system power returns, transition will depend on the state just prior to the entry to G3 and the AFTERG3_EN bit in the GEN_PMCON_3 register (D31:F0, offset A4). Refer to Table 3-27 for more details.

Table 3-21 shows the transitions rules among the various states. Transitions among the various states may appear to temporarily transition through intermediate states. For example, in going from S0 to S3, it may appear to pass through the G1/S1 states. These intermediate transitions and states are not listed in the table.

Table 3-21. State Transition Rules for Intel® Xeon® Processor D-1500 Product Family (Sheet 1 of 2)

Present State	Transition Trigger	Next State
G0/S0/C0	• Internal Msg • SLP_EN bit set • Power Button Override[3] • Mechanical Off/Power Failure	• G0/S0/Cx • G1/Sx or G2/S5 state • G2/S5 • G3
G0/S0/Cx	• Internal Msg • Power Button Override[3] • Mechanical Off/Power Failure	• G0/S0/C0 • S5 • G3
G1/S1 or G1/S3	• Any Enabled Wake Event • Power Button Override[3] • Conditions met as described in Section 3.12.7 • Mechanical Off/Power Failure	• G0/S0/C0[2] • G2/S5 • G3
G1/S4	• Any Enabled Wake Event • Power Button Override[3] • Mechanical Off/Power Failure	• G0/S0/C0[2] • G2/S5 • G3

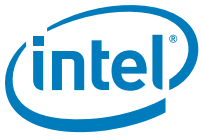


Table 3-21. State Transition Rules for Intel® Xeon® Processor D-1500 Product Family (Sheet 2 of 2)

Present State	Transition Trigger	Next State
G2/S5	• Any Enabled Wake Event • Mechanical Off/Power Failure	• G0/S0/C0[2] • G3
G2	• Any Enabled Wake Event • Mechanical Off/Power Failure	• G0/S0/C0[2] • G1/S3, G1/S4 or G2/S5 (see Section 3.12.7) • G3
G3	• Power Returns	• S0/C0 (reboot) or G2/S5[4] (stay off until power button pressed or other wake event)[1,2]

Notes:
1. Some wake events can be preserved through power failure.
2. N/A
3. Includes all other applicable types of events that force the host into and stay in G2/S5.
4. If the system was in G1/S4 before G3 entry, then the system will go to S0/C0 or G1/S4.

3.12.3 System Power Planes

The system has several independent power planes, as described in Table 3-22. When a particular power plane is shut off, it should go to a 0 V level.

Table 3-22. System Power Plane

Plane	Controlled By	Description
Processor	SLP_S3# signal	The SLP_S3# signal can be used to cut the power to the processor completely.
Main	SLP_S3# signal	When SLP_S3# goes active, power can be shut off to any circuit not required to wake the system from the S3 state. Since the S3 state requires that the memory context be preserved, power must be retained to the main memory. The processor, devices on the PCI bus, LPC I/F, and graphics will typically be shut off when the Main power plane is off, although there may be small subsections powered.
Memory	SLP_S4# signal	When SLP_S4# goes active, power can be shut off to any circuit not required to wake the system from the S4. Since the memory context does not need to be preserved in the S4 state, the power to the memory can also be shut down.
Intel® ME	SLP_A#	This signal is asserted when the manageability platform goes to MOff. Depending on the platform, this pin may be used to control the Intel Management Engine power planes, LAN subsystem power, and the SPI flash power.
LAN	SLP_LAN#	This signal is asserted in Sx/Moff when both host and Intel ME WoL are not supported. This signal can be use to control power to the Intel GbE PHY.
Suspend Well	SLP_SUS#	This signal is asserted when the Sus rails can be externally shut off for enhanced power saving.
DEVICE[n]	Implementation Specific	Individual subsystems may have their own power plane. For example, GPIO signals may be used to control the power to disk drives, audio amplifiers, or the display screen.

3.12.4 SMI# / SCI Generation

Upon any enabled SMI event taking place while the End of SMI (EOS) bit is set, Intel® Xeon® Processor D-1500 Product Family will clear the EOS bit and assert SMI to the processor, which will cause it to enter SMM space. SMI assertion is performed using a Virtual Legacy Wire (VLW) message. Prior system generations (those based upon legacy processors) used an actual SMI# pin.

Once the SMI VLW has been delivered, Intel® Xeon® Processor D-1500 Product Family takes no action on behalf of active SMI events until Host software sets the End of SMI (EOS) bit. At that point, if any SMI events are still active, Intel® Xeon® Processor D-1500 Product Family will send another SMI VLW message.

The SCI is a level-mode interrupt that is typically handled by an ACPI-aware operating system. In non-APIC systems (which is the default), the SCI IRQ is routed to one of the 8259 interrupts (IRQ 9, 10, or 11). The 8259 interrupt controller must be programmed to level mode for that interrupt.

In systems using the APIC, the SCI can be routed to interrupts 9, 10, 11, 20, 21, 22, or 23. The interrupt polarity changes depending on whether it is on an interrupt shareable with a PIRQ or not (see Section 7.1.14). The interrupt remains asserted until all SCI sources are removed.

Table 3-23 shows which events can cause an SMI and SCI. Some events can be programmed to cause either an SMI or SCI. The usage of the event for SCI (instead of SMI) is typically associated with an ACPI-based system. Each SMI or SCI source has a corresponding enable and status bit.

Table 3-23. Causes of SMI and SCI (Sheet 1 of 3)

Cause	SCI	SMI	Additional Enables	Where Reported
PME#	Yes	Yes	PME_EN=1	PME_STS
PME_B0 (Internal, Bus 0, PME-Capable Agents)	Yes	Yes	PME_B0_EN=1	PME_B0_STS
PCI Express* PME Messages	Yes	Yes	PCI_EXP_EN=1 (Not enabled for SMI)	PCI_EXP_STS
PCI Express Hot-Plug Message	Yes	Yes	HOT_PLUG_EN=1 (Not enabled for SMI)	HOT_PLUG_STS
Power Button Press	Yes	Yes	PWRBTN_EN=1	PWRBTN_STS
Power Button Override (Note 7)	Yes	No	None	PRBTNOR_STS
RTC Alarm	Yes	Yes	RTC_EN=1	RTC_STS
Ring Indicate	Yes	Yes	RI_EN=1	RI_STS
ACPI Timer overflow (2.34 sec.)	Yes	Yes	TMROF_EN=1	TMROF_STS
Any GPI[15:0]	Yes	Yes	GPI[x]_Route=10; GPI[x]_EN=1 (SCI) GPI[x]_Route=01; ALT_GPI[x]_SMI_EN=1 (SMI)	GPI[x]_STS ALT_GPI[x]_SMI_STS
GPIO[27]	Yes	Yes	GP27_EN=1	GP27_STS
TCO SCI Logic	Yes	No	TCOSCI_EN=1	TCOSCI_STS
GPIO[17]	Yes	Yes	GPI[17] Route = 10 GP17_EN=1 (SCI); GPI[17]_Route=01 ALT_GP17_SMI_EN=1 (SMI)	GP17_STS ALT_GPI17_SMI_STS

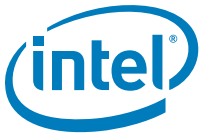


Table 3-23. Causes of SMI and SCI (Sheet 2 of 3)

Cause	SCI	SMI	Additional Enables	Where Reported
GPIO[19]	Yes	Yes	GPI[19] Route = 10 GP19_EN=1 (SCI); GPI[19]_Route=01 ALT_GP19_SMI_EN=1 (SMI)	GP19_STS ALT_GPI19_SMI_STS
GPIO[21]	Yes	Yes	GPI[21] Route=10 GP21_EN=1 (SCI); GPI[21]_Route=01 ALT_GP21_SMI_EN=1 (SMI)	GP21_STS ALT_GPI21_SMI_STS
GPIO[22]	Yes	Yes	GPI[22] Route = 10 GP22_EN=1 (SCI); GPI[22]_Route=01 ALT_GP22_SMI_EN=1 (SMI)	GP22_STS ALT_GPI22_SMI_STS
GPIO[43]	Yes	Yes	GPI[43] Route = 10 GP43_EN=1 (SCI); GPI[43]_Route=01 ALT_GP43_SMI_EN=1 (SMI)	GP43_STS ALT_GPI43_SMI_STS
GPIO[56]	Yes	Yes	GPI[56] Route = 10 GP56_EN=1 (SCI); GPI[56]_Route=01 ALT_GP56_SMI_EN=1 (SMI)	GP56_STS ALT_GPI56_SMI_STS
GPIO[57]	Yes	Yes	GPI[57] Route = 10 GP57_EN=1 (SCI); GPI[57]_Route=01 ALT_GP57_SMI_EN=1 (SMI)	GP57_STS ALT_GPI57_SMI_STS
GPIO[60]	Yes	Yes	GPI[60] Route = 10 GP60_EN=1 (SCI); GPI[60]_Route=01 ALT_GP60_SMI_EN=1 (SMI)	GP60_STS ALT_GPI60_SMI_STS
TCO SCI message from processor	Yes	No	None	BDXSCI_STS
TCO SMI Logic	No	Yes	TCO_EN=1	TCO_STS
TCO SMI –	No	Yes	None	NEWCENTURY_STS
TCO SMI – TCO TIMEROUT	No	Yes	None	TIMEOUT
TCO SMI – OS writes to TCO_DAT_IN register	No	Yes	None	SW_TCO_SMI
TCO SMI – Internal Message	No	Yes	None	BDXSMI_STS
TCO SMI – NMI occurred (and NMIs mapped to SMI)	No	Yes	NMI2SMI_EN=1	NMI2SMI_STS
TCO SMI – INTRUDER# signal goes active	No	Yes	INTRD_SEL=10	INTRD_DET

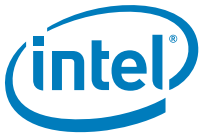
Table 3-23. Causes of SMI and SCI (Sheet 3 of 3)

Cause	SCI	SMI	Additional Enables	Where Reported
TCO SMI – Change of the BIOSWE (D31:F0:DCh, Bit 0) bit from 0 to 1	No	Yes	BLE=1	BIOSWR_STS
TCO SMI – Write attempted to BIOS	No	Yes	BIOSWE=1	BIOSWR_STS
BIOS_RLS written to	Yes	No	GBL_EN=1	GBL_STS
GBL_RLS written to	No	Yes	BIOS_EN=1	BIOS_STS
Write to B2h register	No	Yes	APMC_EN = 1	APM_STS
Periodic timer expires	No	Yes	PERIODIC_EN=1	PERIODIC_STS
64 ms timer expires	No	Yes	SWSMI_TMR_EN=1	SWSMI_TMR_STS
Enhanced USB Legacy Support Event	No	Yes	LEGACY_USB2_EN = 1	LEGACY_USB2_STS
Enhanced USB Intel Specific Event	No	Yes	INTEL_USB2_EN = 1	INTEL_USB2_STS
Serial IRQ SMI reported	No	Yes	None	SERIRQ_SMI_STS
Device monitors match address in its range	No	Yes	None	DEVTRAP_STS
SMBus Host Controller	No	Yes	SMB_SMI_EN Host Controller Enabled	SMBus host status reg.
SMBus Slave SMI message	No	Yes	None	SMBUS_SMI_STS
SMBus SMBALERT# signal active	No	Yes	None	SMBUS_SMI_STS
SMBus Host Notify message received	No	Yes	HOST_NOTIFY_INTREN	SMBUS_SMI_STS HOST_NOTIFY_STS
Access microcontroller 62h/66h	No	Yes	MCSMI_EN	MCSMI_STS
SLP_EN bit written to 1	No	Yes	SLP_SMI_EN=1	SLP_SMI_STS
SPI Command Completed	No	Yes	None	SPI_STS
Software Generated GPE	Yes	Yes	SWGPE_EN=1	SWGPE_STS
USB Per-Port Registers Write Enable bit changes to 1	No	Yes	INTEL_USB2_EN=1, Write_Enable_SMI_Enable=1	INTEL_USB2_STS, Write Enable Status
GPIO Lockdown Enable bit changes from '1' to '0'	No	Yes	GPIO_UNLOCK_SMI_EN=1	GPIO_UNLOCK_SMI_STS
Wake Alarm Device Timer	Yes	Yes	WADT_EN	WADT_STS

Notes:
1. SCI_EN must be 1 to enable SCI, except for BIOS_RLS. SCI_EN must be 0 to enable SMI.
2. SCI can be routed to cause interrupt 9:11 or 20:23 (20:23 only available in APIC mode).
3. GBL_SMI_EN must be 1 to enable SMI.
4. EOS must be written to 1 to re-enable SMI for the next 1.
5. Intel® Xeon® Processor D-1500 Product Family must have SMI fully enabled when Intel® Xeon® Processor D-1500 Product Family is also enabled to trap cycles. If SMI is not enabled in conjunction with the trap enabling, then hardware behavior is undefined.
6. Only GPI[15:0] may generate an SMI or SCI.
7. When a power button override first occurs, the system will transition immediately to S5. The SCI will only occur after the next wake to S0 if the residual status bit (PRBTNOR_STS) is not cleared prior to setting SCI_EN.
8. GBL_STS being set will cause an SCI, even if the SCI_EN bit is not set. Software must take great care not to set the BIOS_RLS bit (which causes GBL_STS to be set) if the SCI handler is not in place.

3.12.4.1 PCI Express SCI

PCI Express ports and the processor have the ability to cause PME using messages. When a PME message is received, Intel® Xeon® Processor D-1500 Product Family will set the PCI_EXP_STS bit. If the PCI_EXP_EN bit is also set, Intel® Xeon® Processor D-1500 Product Family can cause an SCI using the GPE1_STS register.



3.12.4.2 PCI Express* Hot-Plug

PCI Express has a Hot-Plug mechanism and is capable of generating a SCI using the GPE1 register. It is also capable of generating an SMI. However, it is not capable of generating a wake event.

3.12.5 C-States

Intel® Xeon® Processor D-1500 Product Family-based systems implement C-states by having the processor control the states. The chipset exchanges messages with the processor as part of the C-state flow, but the chipset does not directly control any of the processor impacts of C-states, such as voltage levels or processor clocking. In addition to the messages, Intel® Xeon® Processor D-1500 Product Family also provides additional information to the processor using a sideband pin (PMSYNCH). All of the legacy C-state related pins (STPCLK#, STP_CPU#, DPRSLP#, DPRSLPVR#, and so on) do not exist on Intel® Xeon® Processor D-1500 Product Family.

3.12.6 Sleep States

3.12.6.1 Sleep State Overview

Intel® Xeon® Processor D-1500 Product Family directly supports different sleep states (S1–S5), which are entered by methods such as setting the SLP_EN bit or due to a Power Button press. The entry to the Sleep states is based on several assumptions:

- The G3 state cannot be entered using any software mechanism. The G3 state indicates a complete loss of power.

3.12.6.2 Initiating Sleep State

Sleep states (S1–S5) are initiated by:

- Masking interrupts, turning off all bus master enable bits, setting the desired type in the SLP_TYP field, and then setting the SLP_EN bit. The hardware then attempts to gracefully put the system into the corresponding Sleep state.
- Pressing the PWRBTN# Signal for more than 4 seconds to cause a Power Button Override event. In this case the transition to the S5 state is less graceful, since there are no dependencies on internal messages from the processing unit or on clocks other than the RTC clock.
- Assertion of the THRMTRIP# signal will cause a transition to the S5 state. This can occur when system is in S0 or S1 state.
- Shutdown by integrated manageability functions
- Internal watchdog timer time-out events

Table 3-24. Sleep Types

Sleep Type	Comment
S1	System lowers the processor's power consumption. No snooping is possible in this state.
S4	Intel® Xeon® Processor D-1500 Product Family asserts SLP_S3# and SLP_S4#. The SLP_S4# signal shuts off the power to the memory subsystem. Only devices needed to wake from this state should be powered.

3.12.6.3 Exiting Sleep States

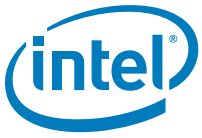
Sleep states (S1–S5) are exited based on Wake events. The Wake events forces the system to a full on state (S0), although some non-critical subsystems might still be shut off and have to be brought back manually. For example, the hard disk may be shut off during a sleep state and have to be enabled using a GPIO pin before it can be used.

Upon exit from Intel® Xeon® Processor D-1500 Product Family-controlled Sleep states, the WAK_STS bit is set. The possible causes of Wake Events (and their restrictions) are shown in Table 3-25.

Table 3-25. Causes of Wake Events

Cause	How Enabled	Wake from S1, Sx	Wake from S1, Sx After Power Loss (Note 1)	Wake from "Reset" Types (Note 2)
RTC Alarm	Set RTC_EN bit in PM1_EN register.	Yes	Yes	No
Power Button	Always enabled as Wake event.	Yes	Yes	Yes
GPI[15:0] GPIO17, GPIO19, GPIO21, GPIO22, GPIO43, GPIO57, GPIO60	GPE0_EN register ***Note:*** GPIs that are in the core well are not capable of waking the system from sleep states when the core well is not powered.	Yes	No	No
GPIO27 (Intel LAN solution uses GPIO27 for PHY Wake)	Set GP27_EN in GPE0_EN Register.	Yes	Yes	Yes
LAN	Will use PME#. Wake enable set with LAN logic.	Yes	Yes	No
RI#	Set RI_EN bit in GPE0_EN register.	Yes	Yes	No
Primary PME#	PME_B0_EN bit in GPE0_EN register.	Yes	Yes	No
Secondary PME#	Set PME_EN bit in GPE0_EN register.	Yes	Yes	No
PCI_EXP_WAKE#	PCI_EXP_WAKE bit. (Note 3)	Yes	Yes	No
SATA	Set PME_EN bit in GPE0_EN register. (Note 4)	Yes (S1 only)	Yes (S1 only)	No
PCI_EXP PME Message	Must use the PCI Express* WAKE# pin rather than messages for wake from S4 or S5.	Yes (S1 only)	Yes (S1 only)	No
SMBALERT#	Always enabled as Wake event.	Yes	Yes	Yes
SMBus Slave Wake Message (01h)	Wake/SMI# command always enabled as a Wake event. ***Note:*** SMBus Slave Message can wake the system from S1–S5, as well as from S5 due to Power Button Override.	Yes	Yes	Yes
SMBus Host Notify message received	HOST_NOTIFY_WKEN bit SMBus Slave Command register. Reported in the SMB_WAK_STS bit in the GPEO_STS register.	Yes	Yes	Yes
Intel® ME Non-Maskable Wake	Always enabled as a wake event.	Yes	Yes	Yes
Integrated WoL Enable Override	WoL Enable Override bit (in Configuration Space).	Yes	Yes	Yes
Wake Alarm Device	WADT_EN in GPE0_EN	Yes	No	No

Notes:
1. This column represents what Intel® Xeon® Processor D-1500 Product Family would honor as wake events but there may be enabling dependencies on the device side which are not enabled after a power loss.



2. Reset Types include: Power Button override, Intel ME initiated power button override, Intel ME initiated host partition reset with power down, Intel ME Watchdog Timer, SMBus unconditional power down, processor thermal trip, Intel® Xeon® Processor D-1500 Product Family catastrophic temperature event.
3. When the WAKE# pin is active and the PCI Express device is enabled to wake the system, Intel® Xeon® Processor D-1500 Product Family will wake the platform.
4. SATA can only trigger a wake event in S1, but if PME is asserted prior to S4/S5 entry and software does not clear the PME_B0_STS, a wake event would still result.

It is important to understand that the various GPIs have different levels of functionality when used as wake events. The GPIs that reside in the core power well can only generate wake events from sleep states where the core well is powered. Also, only certain GPIs are "ACPI Compliant," meaning that their Status and Enable bits reside in ACPI I/O space. Table 3-26 summarizes the use of GPIs as wake events.

Table 3-26. GPI Wake Events

GPI	Power Well	Wake From	Notes
GPI[7:0]	Core	S1	ACPI Compliant
GPI[15:8]	Suspend	S1–S5	ACPI Compliant

The latency to exit the various Sleep states varies greatly and is heavily dependent on power supply design, so much so that the exit latencies due to Intel® Xeon® Processor D-1500 Product Family are insignificant.

3.12.6.4 PCI Express* WAKE# Signal and PME Event Message

PCI Express ports can wake the platform from any sleep state (S1, S4, or S5) using the WAKE# pin. WAKE# is treated as a wake event, but does not cause any bits to go active in the GPE_STS register.

PCI Express ports have the ability to cause PME using messages. When a PME message is received, Intel® Xeon® Processor D-1500 Product Family will set the PCI_EXP_STS bit.

3.12.6.5 Sx-G3-Sx, Handling Power Failures

Depending on when the power failure occurs and how the system is designed, different transitions could occur due to a power failure.

The AFTERG3_EN bit provides the ability to program whether or not the system should boot once power returns after a power loss event. If the policy is to not boot, the system remains in an S5 state (unless previously in S4). There are only three possible events that will wake the system after a power failure.

1. **PWRBTN#:** PWRBTN# is always enabled as a wake event. When RSMRST# is low (G3 state), the PWRBTN_STS bit is reset. When Intel® Xeon® Processor D-1500 Product Family exits G3 after power returns (RSMRST# goes high), the PWRBTN# signal is already high (because V_{CC}-standby goes high before RSMRST# goes high) and the PWRBTN_STS bit is 0.
2. **RI#:** RI# does not have an internal pull-up. Therefore, if this signal is enabled as a wake event, it is important to keep this signal powered during the power loss event. If this signal goes low (active), when power returns the RI_STS bit is set and the system interprets that as a wake event.
3. **RTC Alarm:** The RTC_EN bit is in the RTC well and is preserved after a power loss. Like PWRBTN_STS the RTC_STS bit is cleared when RSMRST# goes low.

Intel® Xeon® Processor D-1500 Product Family monitors both Intel® Xeon® Processor D-1500 Product Family PWROK and RSMRST# to detect for power failures. If Intel® Xeon® Processor D-1500 Product Family PWROK goes low, the PWROK_FLR bit is set. If RSMRST# goes low, PWR_FLR is set.

Note: Although PME_EN is in the RTC well, this signal cannot wake the system after a power loss. PME_EN is cleared by RTCRST#, and PME_STS is cleared by RSMRST#.

Table 3-27. Transitions Due to Power Failure

State at Power Failure	AFTERG3_EN bit	Transition When Power Returns
S0, S1	1 0	S5 S0
S4	1 0	S4 S0
S5	1 0	S5 S0

3.12.7 Event Input Signals and Their Usage

Intel® Xeon® Processor D-1500 Product Family has various input signals that trigger specific events. This section describes those signals and how they should be used.

3.12.7.1 PWRBTN# (Power Button)

Intel® Xeon® Processor D-1500 Product Family PWRBTN# signal operates as a "Fixed Power Button" as described in the *Advanced Configuration and Power Interface, Version 2.0b.* PWRBTN# signal has a 16 ms de-bounce on the input. The state transition descriptions are included in Table 3-28. The transitions start as soon as the PWRBTN# is pressed (but after the debounce logic), and does not depend on when the Power Button is released.

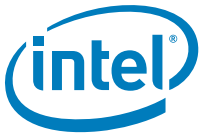
Note: During the time that the SLP_S4# signal is stretched for the minimum assertion width (if enabled), the Power Button is not a wake event. Refer to the following Power Button Override Function section for further details.

Table 3-28. Transitions Due to Power Button

Present State	Event	Transition/Action	Comment
S0/Cx	PWRBTN# goes low	SMI or SCI generated (depending on SCI_EN, PWRBTN_EN and GLB_SMI_EN)	Software typically initiates a Sleep state
S1–S5	PWRBTN# goes low	Wake Event. Transitions to S0 state	Standard wakeup
G3	PWRBTN# pressed	None	No effect since no power Not latched nor detected
S0–S4	PWRBTN# held low for at least 4 consecutive seconds	Unconditional transition to S5 state	No dependence on any subsystem

Power Button Override Function

If PWRBTN# is observed active for at least four consecutive seconds, the state machine should unconditionally transition to the G2/S5 state, regardless of present state (S0–S4), even if Intel® Xeon® Processor D-1500 Product Family PWROK is not active. In



this case, the transition to the G2/S5 state should not depend on any particular response from the processor (such as, Messages), nor any similar dependency from any other subsystem.

The PWRBTN# status is readable to check if the button is currently being pressed or has been released. The status is taken after the de-bounce, and is readable using the PWRBTN_LVL bit.

Note: The 4-second PWRBTN# assertion should only be used if a system lock-up has occurred. The 4-second timer starts counting when Intel® Xeon® Processor D-1500 Product Family is in a S0 state. If the PWRBTN# signal is asserted and held active when the system is in a suspend state (S1–S5), the assertion causes a wake event. Once the system has resumed to the S0 state, the 4-second timer starts.

Note: During the time that the SLP_S4# signal is stretched for the minimum assertion width (if enabled by D31:F0:A4h Bit 3), the Power Button is not a wake event. As a result, it is conceivable that the user will press and continue to hold the Power Button waiting for the system to awake. Since a 4-second press of the Power Button is already defined as an Unconditional Power down, the power button timer will be forced to inactive while the power-cycle timer is in progress. Once the power-cycle timer has expired, the Power Button awakes the system. Once the minimum SLP_S4# power cycle expires, the Power Button must be pressed for another 4 to 5 seconds to create the Override condition to S5.

Sleep Button

The *Advanced Configuration and Power Interface, Version 2.0b* defines an optional Sleep button. It differs from the power button in that it only is a request to go from S0 to S1–S4 (not S5). Also, in an S5 state, the Power Button can wake the system, but the Sleep Button cannot.

Although Intel® Xeon® Processor D-1500 Product Family does not include a specific signal designated as a Sleep Button, one of the GPIO signals can be used to create a "Control Method" Sleep Button. See the *Advanced Configuration and Power Interface, Version 2.0b* for implementation details.

3.12.7.2 RI# (Ring Indicator)

The Ring Indicator can cause a wake event (if enabled) from the S1–S5 states. Table 3-29 shows when the wake event is generated or ignored in different states. If in the G0/S0/Cx states, Intel® Xeon® Processor D-1500 Product Family generates an interrupt based on RI# active, and the interrupt will be set up as a Break event.

Table 3-29. Transitions Due to RI# Signal

Present State	Event	RI_EN	Event
S0	RI# Active	X	Ignored
S1–S5	RI# Active	0 1	Ignored Wake Event

Note: Filtering/Debounce on RI# will not be done in Intel® Xeon® Processor D-1500 Product Family. Can be in modem or external.

3.12.7.3 PME# (PCI Power Management Event)

The PME# signal comes from a PCI Express* device to request that the system be restarted. The PME# signal can generate an SMI#, SCI, or optionally a Wake event. The event occurs when the PME# signal goes from high to low. No event is caused when it goes from low to high.

There is also an internal PME_B0 bit. This is separate from the external PME# signal and can cause the same effect.

3.12.7.4 SYS_RESET# Signal

When the SYS_RESET# pin is detected as active after the 16 ms debounce logic, Intel® Xeon® Processor D-1500 Product Family attempts to perform a "graceful" reset, by waiting up to 25 ms for the SMBus to go idle. If the SMBus is idle when the pin is detected active, the reset occurs immediately; otherwise, the counter starts. If at any point during the count the SMBus goes idle the reset occurs. If, however, the counter expires and the SMBus is still active, a reset is forced upon the system even though activity is still occurring.

Once the reset is asserted, it remains asserted for 5 to 6 ms regardless of whether the SYS_RESET# input remains asserted or not. It cannot occur again until SYS_RESET# has been detected inactive after the debounce logic, and the system is back to a full S0 state with PLTRST# inactive. If bit 3 of the CF9h I/O register is set, then SYS_RESET# will result in a full power cycle reset.

3.12.7.5 THRMTRIP# Signal

If THRMTRIP# goes active, the processor is indicating an overheat condition, and Intel® Xeon® Processor D-1500 Product Family immediately transitions to an S5 state, driving SLP_S3#, SLP_S4#, and setting the CTS bit. The transition looks like a power button override.

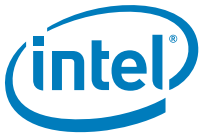
When a THRMTRIP# event occurs, Intel® Xeon® Processor D-1500 Product Family will power down immediately without following the normal S0 -> S5 path. Intel® Xeon® Processor D-1500 Product Family will immediately drive SLP_S3#, and SLP_S4#after sampling THRMTRIP# active.

If the processor is running extremely hot and is heating up, it is possible (although very unlikely) that components around it, such as Intel® Xeon® Processor D-1500 Product Family, are no longer executing cycles properly. Therefore, if THRMTRIP# goes active, and Intel® Xeon® Processor D-1500 Product Family is relying on state machine logic to perform the power down, the state machine may not be working, and the system will not power down.

Intel® Xeon® Processor D-1500 Product Family provides filtering for short low glitches on the THRMTRIP# signal in
order to prevent erroneous system shut downs from noise. Glitches shorter than 25 nsec are ignored.

During boot, THRMTRIP# is ignored until SLP_S3#, PCH_PWROK, and PLTRST# are all '1'. During entry into a powered-down state (due to S4, S5 entry, power cycle reset, and so on) THRMTRIP# is ignored until either SLP_S3# = 0, or Intel® Xeon® Processor D-1500 Product Family PCH_PWROK = 0, or SYS_PWROK = 0.

Note: A thermal trip event will:



- Clear the PWRBTN_STS bit
- Clear all the GPE0_EN register bits
- Clear the SMB_WAK_STS bit only if SMB_SAK_STS was set due to SMBus slave receiving message and not set due to SMBAlert

3.12.8 ALT Access Mode

Before entering a low power state, several registers from powered down parts may need to be saved. In the majority of cases, this is not an issue, as registers have read and write paths. However, several of the ISA compatible registers are either read only or write only. To get data out of write-only registers, and to restore data into read-only registers, Intel® Xeon® Processor D-1500 Product Family implements an ALT access mode.

If the ALT access mode is entered and exited after reading the registers of Intel® Xeon® Processor D-1500 Product Family timer (8254), the timer starts counting faster (13.5 ms). The following steps listed below can cause problems:

1. BIOS enters ALT access mode for reading Intel® Xeon® Processor D-1500 Product Family timer related registers.
2. BIOS exits ALT access mode.
3. BIOS continues through the execution of other needed steps and passes control to the operating system.

After getting control in step #3, if the operating system does not reprogram the system timer again, the timer ticks may be happening faster than expected. For example Microsoft* MS-DOS* and its associated software assume that the system timer is running at 54.6 ms and as a result the time-outs in the software may be happening faster than expected.

Operating systems (such as Microsoft Windows* 98 and Windows* 2000) reprogram the system timer and therefore do not encounter this problem.

For other operating systems (such as Microsoft MS-DOS*), the BIOS should restore the timer back to 54.6 ms before passing control to the operating system. If the BIOS is entering ALT access mode before entering the suspend state it is not necessary to restore the timer contents after the exit from ALT access mode.

3.12.8.1 Write Only Registers with Read Paths in ALT Access Mode

The registers described in Table 3-30 have read paths in ALT access mode. The access number field in the table indicates which register will be returned per access to that port.

Table 3-30. Write Only Registers with Read Paths in ALT Access Mode (Sheet 1 of 2)

Restore Data				Restore Data			
I/O Addr	# of Rds	Access	Data	I/O Addr	# of Rds	Access	Data
00h	2	1	DMA Chan 0 base address low byte	40h	7	1	Timer Counter 0 status, bits [5:0]
		2	DMA Chan 0 base address high byte			2	Timer Counter 0 base count low byte
01h	2	1	DMA Chan 0 base count low byte			3	Timer Counter 0 base count high byte
		2	DMA Chan 0 base count high byte			4	Timer Counter 1 base count low byte
02h	2	1	DMA Chan 1 base address low byte			5	Timer Counter 1 base count high byte
		2	DMA Chan 1 base address high byte			6	Timer Counter 2 base count low byte
03h	2	1	DMA Chan 1 base count low byte			7	Timer Counter 2 base count high byte
		2	DMA Chan 1 base count high byte	41h	1		Timer Counter 1 status, bits [5:0]
04h	2	1	DMA Chan 2 base address low byte	42h	1		Timer Counter 2 status, bits [5:0]
		2	DMA Chan 2 base address high byte	70h	1		Bit 7 = NMI Enable, Bits [6:0] = RTC Address
05h	2	1	DMA Chan 2 base count low byte	C4h	2	1	DMA Chan 5 base address low byte
		2	DMA Chan 2 base count high byte			2	DMA Chan 5 base address high byte
06h	2	1	DMA Chan 3 base address low byte	C6h	2	1	DMA Chan 5 base count low byte
		2	DMA Chan 3 base address high byte			2	DMA Chan 5 base count high byte
07h	2	1	DMA Chan 3 base count low byte	C8h	2	1	DMA Chan 6 base address low byte
		2	DMA Chan 3 base count high byte			2	DMA Chan 6 base address high byte
08h	6	1	DMA Chan 0–3 Command[2]	CAh	2	1	DMA Chan 6 base count low byte
		2	DMA Chan 0–3 Request			2	DMA Chan 6 base count high byte
		3	DMA Chan 0 Mode: Bits(1:0) = 00	CCh	2	1	DMA Chan 7 base address low byte
		4	DMA Chan 1 Mode: Bits(1:0) = 01			2	DMA Chan 7 base address high byte
		5	DMA Chan 2 Mode: Bits(1:0) = 10	CEh	2	1	DMA Chan 7 base count low byte
		6	DMA Chan 3 Mode: Bits(1:0) = 11.			2	DMA Chan 7 base count high byte

Table 3-30. Write Only Registers with Read Paths in ALT Access Mode (Sheet 2 of 2)

Restore Data				Restore Data			
I/O Addr	# of Rds	Access	Data	I/O Addr	# of Rds	Access	Data
20h	12	1	PIC ICW2 of Master controller	D0h	6	1	DMA Chan 4–7 Command[2]
		2	PIC ICW3 of Master controller			2	DMA Chan 4–7 Request
		3	PIC ICW4 of Master controller			3	DMA Chan 4 Mode: Bits(1:0) = 00
		4	PIC OCW1 of Master controller[1]			4	DMA Chan 5 Mode: Bits(1:0) = 01
		5	PIC OCW2 of Master controller			5	DMA Chan 6 Mode: Bits(1:0) = 10
		6	PIC OCW3 of Master controller			6	DMA Chan 7 Mode: Bits(1:0) = 11.
		7	PIC ICW2 of Slave controller				
		8	PIC ICW3 of Slave controller				
		9	PIC ICW4 of Slave controller				
		10	PIC OCW1 of Slave controller[1]				
		11	PIC OCW2 of Slave controller				
		12	PIC OCW3 of Slave controller				

Notes:
1. The OCW1 register must be read before entering ALT access mode.
2. Bits 5, 3, 1, and 0 return 0.

3.12.8.2 PIC Reserved Bits

Many bits within the PIC are reserved, and must have certain values written in order for the PIC to operate properly. Therefore, there is no need to return these values in ALT access mode. When reading PIC registers from 20h and A0h, the reserved bits shall return the values listed in Table 3-31.

Table 3-31. PIC Reserved Bits Return Values

PIC Reserved Bits	Value Returned
ICW2(2:0)	000
ICW4(7:5)	000
ICW4(3:2)	00
ICW4(0)	0
OCW2(4:3)	00
OCW3(7)	0
OCW3(5)	Reflects bit 6
OCW3(4:3)	01

3.12.8.3 Read Only Registers with Write Paths in ALT Access Mode

The registers described in Table 3-32 have write paths to them in ALT access mode. Software restores these values after returning from a powered down state. These registers must be handled special by software. When in normal mode, writing to the base address/count register also writes to the current address/count register. Therefore, the base address/count must be written first, then the part is put into ALT access mode and the current address/count register is written.

Table 3-32. Register Write Accesses in ALT Access Mode

I/O Address	Register Write Value
08h	DMA Status Register for Channels 0–3
D0h	DMA Status Register for Channels 4–7

3.12.9 System Power Supplies, Planes, and Signals

3.12.9.1 Power Plane Control with SLP_S3#, SLP_S4#, SLP_A# and SLP_LAN#

The SLP_S3# output signal can be used to cut power to the system core supply, since it only goes active for the Suspend-to-RAM state (typically mapped to ACPI S3). Power must be maintained to Intel® Xeon® Processor D-1500 Product Family suspend well, and to any other circuits that need to generate Wake signals from the Suspend-to-RAM state.

Cutting power to the core may be done using the power supply, or by external FETs on the motherboard.

The SLP_S4# output signal can be used to cut power to the system core supply, as well as power to the system memory, since the context of the system is saved on the disk. Cutting power to the memory may be done using the power supply, or by external FETs on the motherboard.

The SLP_S4# output signal is used to remove power to additional subsystems that are powered during SLP_S3#.

SLP_A# output signal can be used to cut power to the Intel Management Engine and SPI flash on a platform that supports the M3 state.

SLP_LAN# output signal can be used to cut power to the external Clarkville GbE PHY device.

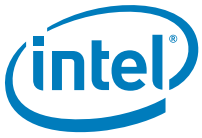
3.12.9.2 SLP_S4# and Suspend-To-RAM Sequencing

The system memory suspend voltage regulator is controlled by the Glue logic. The SLP_S4# signal should be used to remove power to system memory rather than the SLP_S5# signal. The SLP_S4# logic in Intel® Xeon® Processor D-1500 Product Family provides a mechanism to fully cycle the power to the DRAM and/or detect if the power is not cycled for a minimum time.

Note: To use the minimum DRAM power-down feature that is enabled by the SLP_S4# Assertion Stretch Enable bit (D31:F0:A4h Bit 3), the DRAM power must be controlled by the SLP_S4# signal.

3.12.9.3 PCH_PWROK Signal

When asserted, PCH_PWROK is an indication to Intel® Xeon® Processor D-1500 Product Family that its core well power rails are powered and stable. PCH_PWROK can be driven asynchronously. When Intel® Xeon® Processor D-1500 Product Family PCH_PWROK is low, Intel® Xeon® Processor D-1500 Product Family asynchronously asserts PLTRST#. PCH_PWROK must not glitch, even if RSMRST# is low.



It is required that the power associated with PCIe* have been valid for 99 ms prior to PCH_PWROK assertion in order to comply with the 100 ms PCIe 2.0 specification on PLTRST# de-assertion.

Note: SYS_RESET# is recommended for implementing the system reset button. This saves external logic that is needed if the PCH_PWROK input is used. Additionally, it allows for better handling of the SMBus and processor resets and avoids improperly reporting power failures.

3.12.9.4 SLP_LAN# Pin Behavior

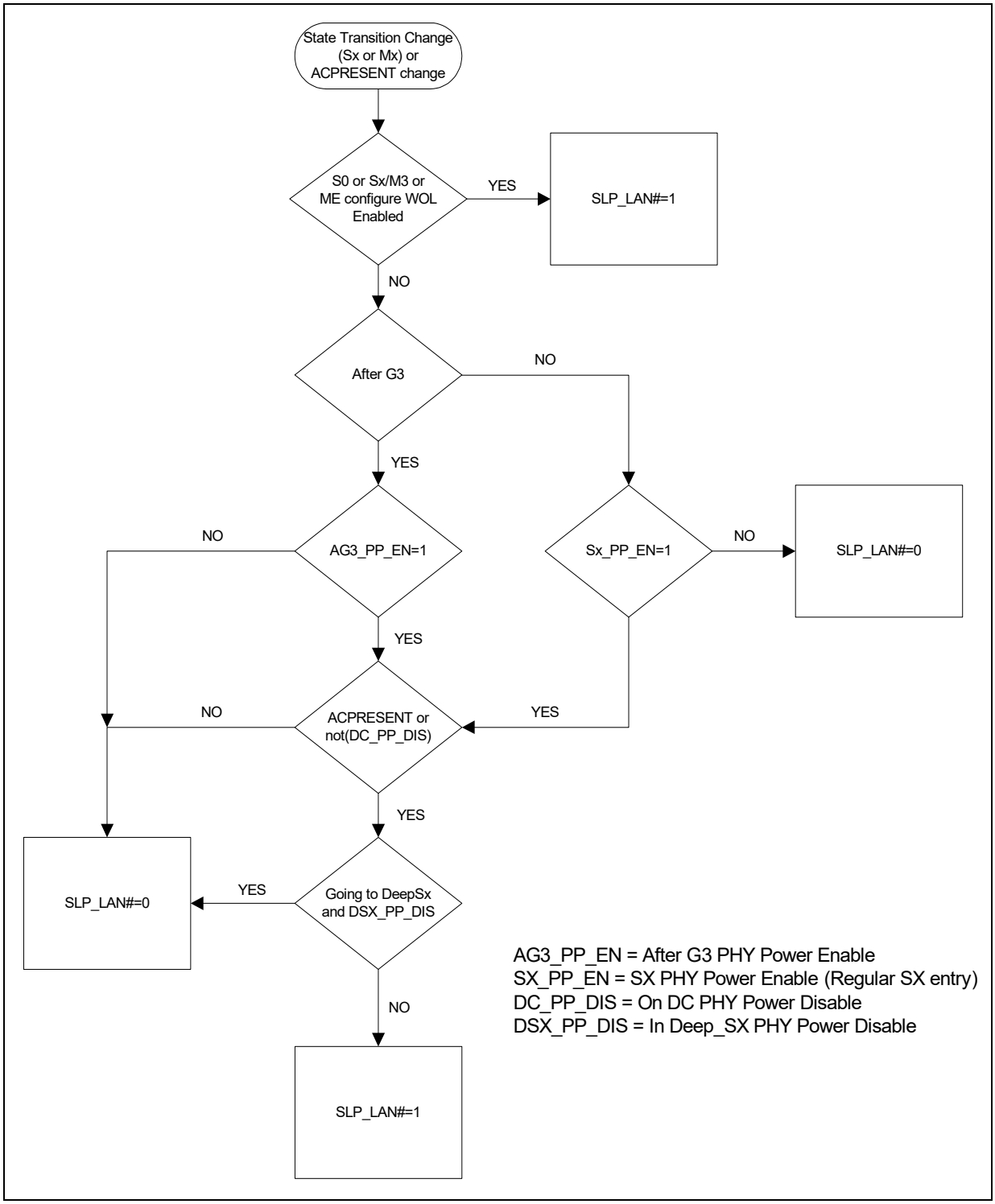
Intel® Xeon® Processor D-1500 Product Family controls the voltage rails into the external LAN PHY using the
SLP_LAN# pin.

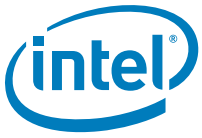
- The LAN PHY is always powered when the Host & ME systems are running.
  - SLP_LAN#='1' whenever SLP_S3#='1' or SLP_A#='1'.
- If the LAN PHY is required by ME in Sx/Moff, ME must configure SLP_LAN#='1' irrespective of the power source and the destination power state. ME must be powered at least once after G3 to configure this.
- If the LAN PHY is required after a G3 transition, the host BIOS must set AG3_PP_EN (B0:D31:F0:A2h bit 12).
- If the LAN PHY is required in Sx/Moff, the host BIOS must set SX_PP_EN (B0:D31:F0:A2h bit 11).
- If the LAN PHY is not required if the source of power is battery, the host BIOS must set DC_PP_DIS (B0:D31:F0:A2h bit 14).

Note: Intel® ME configuration of SLP_LAN# in Sx/Moff is dependent on Intel® ME power policy configuration.

The flow chart below shows how a decision is made to drive SLP_LAN# every time its policy needs to be evaluated.

Figure 3-5. Conceptual Diagram of SLP_LAN#





3.12.9.5 SLP_WLAN# Pin Behavior

Intel® Xeon® Processor D-1500 Product Family controls the voltage rails into the external wireless LAN PHY using the SLP_WLAN# pin.

- The wireless LAN PHY is always powered when the Host is running.
  - SLP_WLAN#='1' whenever SLP_S3#='1'.
- If Wake on Wireless LAN (WoWLAN) is required from S4/S5 states, the host BIOS must set HOST_WLAN_PP_EN (RCBA+3318h bit 4).
- If Intel® ME has access to the Wireless LAN device
  - The Wireless LAN device must always be powered as long as Intel® ME is powered. SLP_WLAN#='1' whenever SLP_A#='1'.
  - If Wake on Wireless LAN (WoWLAN) is required from Moff state, Intel® ME will configure SLP_WLAN#='1' in Sx/Moff.

Intel® ME configuration of SLP_WLAN# in Sx/Moff is dependent on Intel® ME power policy configuration.

3.12.9.6 SUSPWRDNACK / SUSWARN# / GPIO30 Steady State Pin Behavior

The following tables summarize SUSPWRDNACK/SUSWARN#/GPIO30 Pin Behavior.

Table 3-33. SUSPWRDNACK / SUSWARN# / GPIO30 Pin Behavior

	GPIO30 Setting	Pin Value in S0	Pin Value in Sx/Moff	Pin Value in Sx/M3
SUSPWRDNACK	Native	0	Depends on ME power package and source (note 1)	0
SUSWARN#	Native	1	1 (note 2)	1
GPIO30	IN	High-Z	High-Z	High-Z
	OUT	Depends on GPIO30 output data value	Depends on GPIO30 output data value	Depends on GPIO30 output data value

Notes:
1. Intel® Xeon® Processor D-1500 Product Family will drive SPDA pin based on Intel® ME power policy configuration.

Table 3-34. SUSPWRDNACK during Reset

PIC Reserved Bits	Value Returned
Power Cycle Reset	0
Global Reset	0
Straight to S5	Intel® Xeon® Processor D-1500 Product Family initially drive to '0' and then drive per ME power policy configuration.

3.12.9.7 RTCRST# and SRTCRST#

RTCRST# is used to reset Intel® Xeon® Processor D-1500 Product Family registers in the RTC Well to their default value. If a jumper is used on this pin, it should only be pulled low when system is in the G3 state and then replaced to the default jumper position. Upon booting, BIOS should recognize that RTCRST# was asserted and clear internal Intel® Xeon® Processor D-1500 Product Family registers accordingly. It is imperative that this signal not be pulled low in the S0 to S5 states.

SRTCRST# is used to reset portions of the Intel® Management Engine and should not be connected to a jumper or button on the platform. The only time this signal gets asserted (driven low in combination with RTCRST#) should be when the coin cell battery is removed or not installed and the platform is in the G3 state. Pulling this signal low independently (without RTCRST# also being driven low) may cause the platform to enter an indeterminate state. Similar to RTCRST#, it is imperative that SRTCRST# not be pulled low in the S0 to S5 states.

3.12.10 Legacy Power Management Theory of Operation

Instead of relying on ACPI software, legacy power management uses BIOS and various hardware mechanisms. The scheme relies on the concept of detecting when individual subsystems are idle, detecting when the whole system is idle, and detecting when accesses are attempted to idle subsystems.

However, the operating system is assumed to be at least APM enabled. Without APM calls, there is no quick way to know when the system is idle between keystrokes. Intel® Xeon® Processor D-1500 Product Family does not support burst modes.

3.12.10.1 APM Power Management

Intel® Xeon® Processor D-1500 Product Family has a timer that, when enabled by the 1MIN_EN bit in the SMI Control and Enable register, generates an SMI once per minute. The SMI handler can check for system activity by reading the DEVTRAP_STS register. If none of the system bits are set, the SMI handler can increment a software counter. When the counter reaches a sufficient number of consecutive minutes with no activity, the SMI handler can then put the system into a lower power state.

If there is activity, various bits in the DEVTRAP_STS register will be set. Software clears the bits by writing a 1 to the bit position.

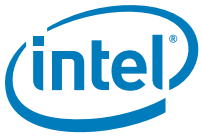
The DEVTRAP_STS register allows for monitoring various internal devices, or Super I/O devices (SP, PP, FDC) on LPC, keyboard controller accesses, or audio functions on LPC.

3.12.11 Reset Behavior

When a reset is triggered, Intel® Xeon® Processor D-1500 Product Family will send a warning message to the processor to allow the processor to attempt to complete any outstanding memory cycles and put memory into a safe state before the platform is reset. When the processor is ready, it will send an acknowledge message to Intel® Xeon® Processor D-1500 Product Family. Once the message is received, Intel® Xeon® Processor D-1500 Product Family asserts PLTRST#.

Intel® Xeon® Processor D-1500 Product Family does not require an acknowledge message from the processor to trigger PLTRST#. A global reset will occur after 4 seconds if an acknowledge from the processor is not received.

A reset in which the host platform is reset and PLTRST# is asserted is called a Host Reset or Host Partition Reset. Depending on the trigger, a host reset may also result in power cycling (see Table 3-35 for details). If a host reset is triggered and Intel® Xeon® Processor D-1500 Product Family times out before receiving an acknowledge message from the processor, a Global Reset with power cycle will occur.



A reset in which the host and Intel® ME partitions of the platform are reset is called a Global Reset. During a Global Reset, all Intel® Xeon® Processor D-1500 Product Family functionality is reset except RTC Power Well backed information and Suspend well status, configuration, and functional logic for controlling and reporting the reset. Intel ME and Host power back up after the power
cycle period.

Straight to S5 is another reset type where all power wells that are controlled by the SLP_S3#, SLP_S4#, and SLP_A# pins, as well as SLP_S5# and SLP_LAN# (if pins are not configured as GPIOs), are turned off. All Intel® Xeon® Processor D-1500 Product Family functionality is reset, except RTC Power Well backed information and Suspend well status, configuration, and functional logic for controlling and reporting the reset. The host stays there until a valid wake event occurs.

Table 3-35 shows the various reset triggers.

Table 3-35. Causes of Host and Global Resets (Sheet 1 of 2)

Trigger	Host Reset without Power Cycle[1]	Host Reset with Power Cycle[2]	Global Reset with Power Cycle[3]	Straight to S5 (Host Stays there)
Write of 0Eh to CF9h (RST_CNT Register)	No	Yes	No (Note 4)	
Write of 06h to CF9h (RST_CNT Register)	Yes	No	No (Note 4)	
SYS_RESET# Asserted and CF9h (RST_CNT Register) Bit 3 = 0	Yes	No	No (Note 4)	
SYS_RESET# Asserted and CF9h (RST_CNT Register) Bit 3 = 1	No	Yes	No (Note 4)	
SMBus Slave Message received for Reset with Power Cycle	No	Yes	No (Note 4)	
SMBus Slave Message received for Reset without Power Cycle	Yes	No	No (Note 4)	
SMBus Slave Message received for unconditional Power Down	No	No	No	Yes
TCO Watchdog Timer reaches zero two times	Yes	No	No (Note 4)	
Power Failure: PCH_PWROK signal goes inactive in S0/S1 or DPWROK drops	No	No	Yes	
SYS_PWROK Failure: SYS_PWROK signal goes inactive in S0/S1	No	No	Yes	
Processor Thermal Trip (THRMTRIP#) causes transition to S5 and reset asserts	No	No	No	Yes
Intel® Xeon® Processor D-1500 Product Family internal thermal sensors signals a catastrophic temperature condition	No	No	No	Yes
Power Button 4 second override causes transition to S5 and reset asserts	No	No	No	Yes
Special shutdown cycle from processor causes CF9h-like PLTRST# and CF9h (RST_CNT Register) Bit 3 = 1	No	Yes	No (Note 4)	
Special shutdown cycle from processor causes CF9h-like PLTRST# and CF9h (RST_CNT Register) Bit 3 = 0	Yes	No	No (Note 4)	
Intel® Management Engine Triggered Host Reset without power cycle	Yes	No	No (Note 4)	
Intel® Management Engine Triggered Host Reset with power cycle	No	Yes	No (Note 4)	
Intel® Management Engine Triggered Power Button Override	No	No	No	Yes
Intel® Management Engine Watchdog Timer Timeout	No	No	No	Yes

Table 3-35. Causes of Host and Global Resets (Sheet 2 of 2)

Trigger	Host Reset without Power Cycle[1]	Host Reset with Power Cycle[2]	Global Reset with Power Cycle[3]	Straight to S5 (Host Stays there)
Intel® Management Engine Triggered Global Reset	No	No	Yes	
Intel® Management Engine Triggered Host Reset with power down (host stays there)	No	Yes (Note 5)	No (Note 4)	
PLTRST# Entry Time-out	No	No	Yes	
S4/5 Entry Timeout	No	No	No	Yes
PROCPWRGD Stuck Low	No	No	Yes	
Power Management Watchdog Timer	No	No	No	Yes
Intel® Management Engine Hardware Uncorrectable Error	No	No	No	Yes

Notes:
1. Intel® Xeon® Processor D-1500 Product Family drops this type of reset request if received while the system is in S4/S5.
2. Intel® Xeon® Processor D-1500 Product Family does not drop this type of reset request if received while system is in a software-entered S4/S5 state. However, Intel® Xeon® Processor D-1500 Product Family will perform the reset without executing the RESET_WARN protocol in these states.
3. Intel® Xeon® Processor D-1500 Product Family does not send warning message to processor, reset occurs without delay.
4. Trigger will result in Global Reset with power cycle if the acknowledge message is not received by Intel® Xeon® Processor D-1500 Product Family.
5. Intel® Xeon® Processor D-1500 Product Family waits for enabled wake event to complete reset.

3.13 System Management (D31:F0)

Intel® Xeon® Processor D-1500 Product Family provides various functions to make a system easier to manage and to lower the Total Cost of Ownership (TCO) of the system. Features and functions can be augmented using external A/D converters and GPIO, as well as an external microcontroller.

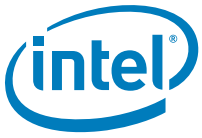
The following features and functions are supported by Intel® Xeon® Processor D-1500 Product Family:

- Processor present detection
  - Detects if processor fails to fetch the first instruction after reset
- Various Error detection (such as ECC Errors) indicated by host controller
  - Can generate SMI#, SCI, SERR, NMI, or TCO interrupt
- Intruder Detect input
  - Can generate TCO interrupt or SMI# when the system cover is removed
  - INTRUDER# allowed to go active in any power state, including G3
- Detection of bad BIOS Flash (FWH or Flash on SPI) programming
  - Detects if data on first read is FFh (indicates that BIOS flash is not programmed)

Note: Voltage ID from the processor can be read using GPI signals.

3.13.1 Theory of Operation

The System Management functions are designed to allow the system to diagnose failing subsystems. The intent of this logic is that some of the system management functionality can be provided without the aid of an external microcontroller.



3.13.1.1 Detecting a System Lockup

When the processor is reset, it is expected to fetch its first instruction. If the processor fails to fetch the first instruction after reset, the TCO timer times out twice and Intel® Xeon® Processor D-1500 Product Family asserts PLTRST#.

3.13.1.2 Handling an Intruder

Intel® Xeon® Processor D-1500 Product Family has an input signal, INTRUDER#, that can be attached to a switch that is activated by the system's case being open. This input has a two RTC clock debounce. If INTRUDER# goes active (after the debouncer), this will set the INTRD_DET bit in the TCO2_STS register. The INTRD_SEL bits in the TCO_CNT register can enable Intel® Xeon® Processor D-1500 Product Family to cause an SMI# or interrupt. The BIOS or interrupt handler can then cause a transition to the S5 state by writing to the SLP_EN bit.

The software can also directly read the status of the INTRUDER# signal (high or low) by clearing and then reading the INTRD_DET bit. This allows the signal to be used as a GPI if the intruder function is not required.

If the INTRUDER# signal goes inactive some point after the INTRD_DET bit is written as a 1, then the INTRD_DET bit will go to a 0 when INTRUDER# input signal goes inactive. This is slightly different than a classic sticky bit, since most sticky bits would remain active indefinitely when the signal goes active and would immediately go inactive when a 1 is written to the bit.

Note: The INTRD_DET bit resides in Intel® Xeon® Processor D-1500 Product Family's RTC well, and is set and cleared synchronously with the RTC clock. Thus, when software attempts to clear INTRD_DET (by writing a 1 to the bit location) there may be as much as two RTC clocks (about 65 µs) delay before the bit is actually cleared. Also, the INTRUDER# signal should be asserted for a minimum of 1 ms to ensure that the INTRD_DET bit will be set.

Note: If the INTRUDER# signal is still active when software attempts to clear the INTRD_DET bit, the bit remains set and the SMI is generated again immediately. The SMI handler can clear the INTRD_SEL bits to avoid further SMIs. However, if the INTRUDER# signal goes inactive and then active again, there will not be further SMIs, since the INTRD_SEL bits would select that no SMI# be generated.

3.13.1.3 Detecting Improper Flash Programming

Intel® Xeon® Processor D-1500 Product Family can detect the case where the BIOS flash is not programmed. This results in the first instruction fetched to have a value of FFh. If this occurs, Intel® Xeon® Processor D-1500 Product Family sets the BAD_BIOS bit. The BIOS flash may reside in FWH or flash on the SPI bus.

3.13.1.4 Heartbeat and Event Reporting using SMLink/SMBus

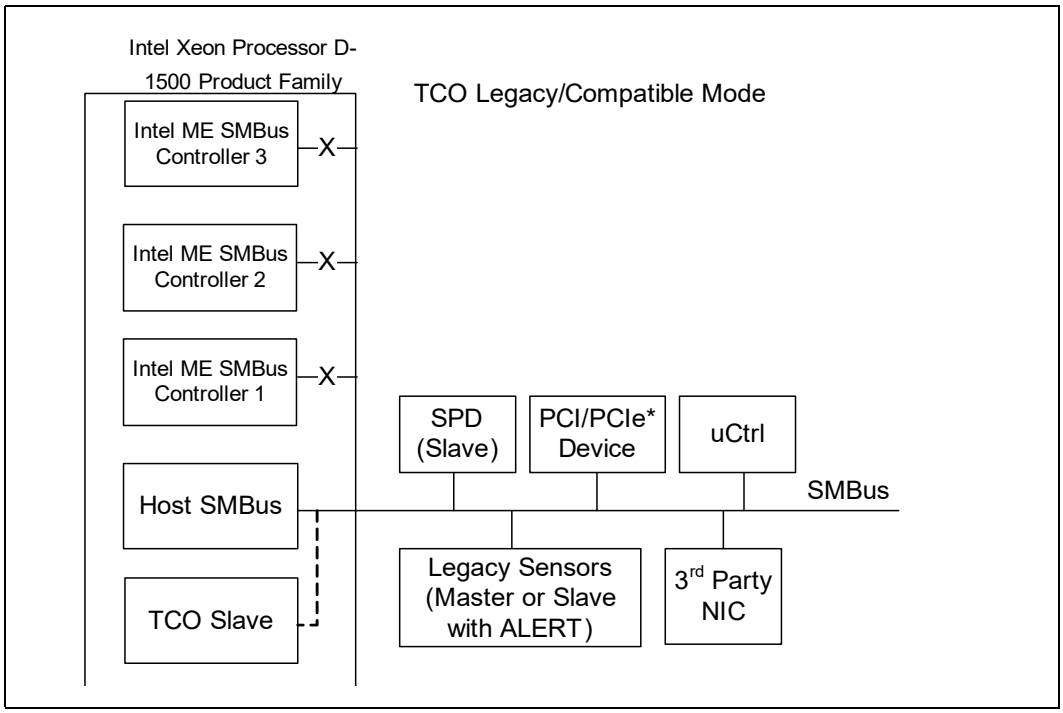
Heartbeat and event reporting using SMLink/SMBus is no longer supported. The Intel® AMT logic in Intel® Xeon® Processor D-1500 Product Family can be programmed to generate an interrupt to the Intel® Management Engine (Intel® ME) when an event occurs. The Intel® ME will poll the TCO registers to gather appropriate bits to send the event message to the Gigabit Ethernet controller, if the Intel® ME is programmed to do so.

3.13.2 TCO Modes

3.13.2.1 TCO Legacy / Compatible Mode

In TCO Legacy/Compatible mode, only the host SMBus is used. The TCO Slave is connected to the host SMBus internally by default. In this mode, the Intel® ME SMBus controllers are not used and should be disabled by soft strap.

Figure 3-6. TCO Legacy/Compatible Mode SMBus Configuration

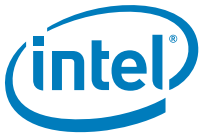


In TCO Legacy/Compatible mode Intel® Xeon® Processor D-1500 Product Family can function directly with an external LAN controller or equivalent external LAN controller to report messages to a network management console without the aid of the system processor. This is crucial in cases where the processor is malfunctioning or cannot function due to being in a low-power state. Table 3-36 includes a list of events that will report messages to the network management console.

Table 3-36. Event Transitions that Cause Messages

Event	Assertion?	De-assertion?	Comments
INTRUDER# pin	Yes	No	Must be in "S1 or hung S0" state
THRM# pin	Yes	Yes	Must be in "S1 or hung S0" state. The THRM# pin is isolated when the core power is off, thus preventing this event in S4–S5.
Watchdog Timer Expired	Yes	No (NA)	"S1 or hung S0" state entered
GPIO[11]/ SMBALERT# pin	Yes	Yes	Must be in "S1 or hung S0" state
CPU_PWR_FLR	Yes	No	"S1 or hung S0" state entered

Note: The GPIO11/SMBALERT# pin will trigger an event message (when enabled by the GPIO11_ALERT_DISABLE bit) regardless of whether it is configured as a GPI or not.



3.13.2.2 Advanced TCO Mode

Intel® Xeon® Processor D-1500 Product Family supports the Advanced TCO mode in which SMLink0 and SMLink1 are used in addition to the host SMBus. In this mode, the Intel ME SMBus controllers must be enabled by soft strap in the flash descriptor.

3.14 General Purpose I/O (D31:F0)

Intel® Xeon® Processor D-1500 Product Family contains up to 68 General Purpose Input/Output (GPIO) signals for Intel® Xeon® Processor D-1500 Product Family. Each GPIO can be configured as an input or output signal. The number of inputs and outputs varies depending on the configuration. Following is a brief summary of GPIO features.

- Capability to mask Suspend well GPIOs from CF9h events (configured using GP_RST_SEL registers)
- Added capability to program GPIO prior to switching to output

3.14.1 Power Wells

Some GPIOs exist in the suspend power plane. Care must be taken to make sure GPIO signals are not driven high into powered-down planes. Some Intel® Xeon® Processor D-1500 Product Family GPIOs may be connected to pins on devices that exist in the core well. If these GPIOs are outputs, there is a danger that a loss of core power (PCH_PWROK low) or a Power Button Override
event results in Intel® Xeon® Processor D-1500 Product Family driving a pin to a logic 1 to another device that is powered down.

3.14.2 SMI# SCI and NMI Routing

The routing bits for GPIO[15:0] allow an input to be routed to SMI#, SCI, NMI or neither. A bit can be routed to either an SMI# or an SCI, but not both.

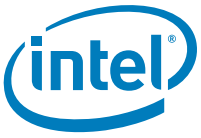
3.14.3 Triggering

GPIO[15:0] have “sticky” bits on the input. Refer to the GPE0_STS register and the ALT_GPI_SMI_STS register. As long as the signal goes active for at least 2 clock cycles, Intel® Xeon® Processor D-1500 Product Family keeps the sticky status bit active. The active level can be selected in the GP_INV register. This does not apply to GPI_NMI_STS residing in GPIO I/O space.

If the system is in an S0 or an S1 state, the GPI inputs are sampled at 33 MHz, so the signal only needs to be active for about 60 ns to be latched. In the S4–S5 states, the GPI inputs are sampled at 32.768 kHz, and thus must be active for at least
61 microseconds to
be latched.

Note: GPIs that are in the core well are not capable of waking the system from sleep states where the core well is not powered.

If the input signal is still active when the latch is cleared, it will again be set. Another edge trigger is not required. This makes these signals “level” triggered inputs.



3.14.4 GPIO Registers Lockdown

The following GPIO registers are locked down when the GPIO Lockdown Enable (GLE) bit is set. The GLE bit resides in D31:F0:GPIO Control (GC) register.

- Offset 00h: GPIO_USE_SEL[31:0]
- Offset 04h: GP_IO_SEL[31:0]
- Offset 0Ch: GP_LVL[31:0]
- Offset 28h: GPI_NMI_EN[15:0]
- Offset 2Ch: GPI_INV[31:0]
- Offset 30h: GPIO_USE_SEL2[63:32]
- Offset 34h: GPI_IO_SEL2[63:32]
- Offset 38h: GP_LVL2[63:32]
- Offset 40h: GPIO_USE_SEL3[95:64]
- Offset 44h: GPI_IO_SEL3[95:64]
- Offset 48h: GP_LVL3[95:64]
- Offset 60h: GP_RST_SEL[31:0]
- Offset 64h: GP_RST_SEL2[63:32]
- Offset 68h: GP_RST_SEL3[95:64]

Note: All other GPIO registers not listed here are not to be locked by GLE.

Once these registers are locked down, they become Read-Only registers and any software writes to these registers will have no effect. To unlock the registers, the GPIO Lockdown Enable (GLE) bit is required to be cleared to '0'. When the GLE bit changes from a '1' to a '0' a System Management Interrupt (SMI#) is generated if enabled. Once the GPIO_UNLOCK_SMI bit is set, it can not be changed until a PLTRST# occurs. This ensures that only BIOS can change the GPIO configuration. If the GLE bit is cleared by unauthorized software, BIOS will set the GLE bit again when the SMI# is triggered and these registers will continue to be locked down.

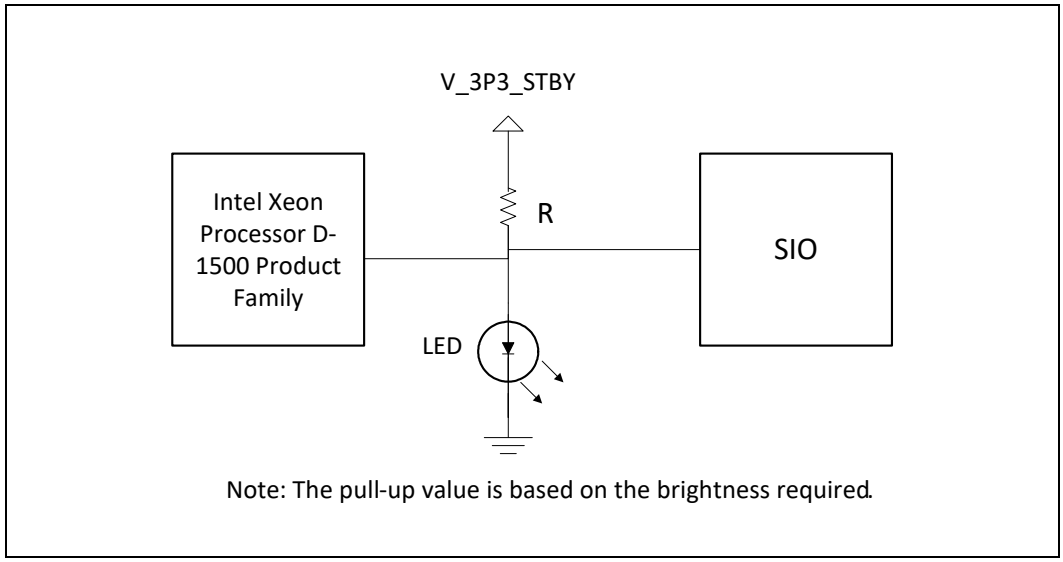
3.14.5 Serial POST Codes over GPIO

Intel® Xeon® Processor D-1500 Product Family adds the extended capability allowing system software to serialize POST or other messages on GPIO. This capability negates the requirement for dedicated diagnostic LEDs on the platform.

3.14.5.1 Theory of Operation

For Intel® Xeon® Processor D-1500 Product Family generation POST code serialization logic will be shared with GPIO. These GPIOs will likely be shared with LED control offered by the Super I/O (SIO) component. Figure 3-7 shows a likely configuration.

Figure 3-7. Serial Post over GPIO Reference Circuit



The anticipated usage model is that either Intel® Xeon® Processor D-1500 Product Family or the SIO can drive a pin low to turn off an LED. In the case of the power LED, the SIO would normally leave its corresponding pin in a high-Z state to allow the LED to turn on. In this state, Intel® Xeon® Processor D-1500 Product Family can blink the LED by driving its corresponding pin low and subsequently tri-stating the buffer. The I/O buffer should not drive a '1' when configured for this functionality and should be capable of sinking 24 mA of current.

An external optical sensing device can detect the on/off state of the LED. By externally post-processing the information from the optical device, the serial bit stream can be recovered. The hardware will supply a 'sync' byte before the actual data transmission to allow external detection of the transmit frequency. The frequency of transmission should be limited to 1 transition every 1 μs to ensure the detector can reliably sample the on/off state of the LED. To allow flexibility in pull-up resistor values for power optimization, the frequency of the transmission is programmable using the DRS field in the GP_GB_CMDSTS register.

The serial bit stream is Manchester encoded. This choice of transmission ensures that a transition will be seen on every clock. The 1 or 0 data is based on the transmission happening during the high or low phase of the clock.

As the clock will be encoded within the data stream, hardware must ensure that the Z-0 and 0-Z transitions are glitch-free. Driving the pin directly from a flop or through glitch-free logic are possible methods to meet the glitch-free requirement.

A simplified hardware/software register interface provides control and status information to track the activity of this block. Software enabling the serial blink capability should implement an algorithm referenced below to send the serialized message on the enabled GPIO.

1. Read the Go/Busy status bit in the GP_GB_CMDSTS register and verify it is cleared. This will ensure that the GPIO is idled and a previously requested message is still not in progress.
2. Write the data to serialize into the GP_GB_DATA register.

3. Write the DLS and DRS values into the GP_GB_CMDSTS register and set the Go bit. This may be accomplished using a single write.

The reference diagram shows the LEDs being powered from the suspend supply. By providing a generic capability that can be used both in the main and the suspend power planes maximum flexibility can be achieved. A key point to make is that Intel® Xeon® Processor D-1500 Product Family will not unintentionally drive the LED control pin low unless a serialization is in progress. System board connections utilizing this serialization capability are required to use the same power plane controlling the LED as Intel® Xeon® Processor D-1500 Product Family GPIO pin. Otherwise, Intel® Xeon® Processor D-1500 Product Family GPIO may float low during the message and prevent the LED from being controlled from the SIO. The hardware will only be serializing messages when the core power well is powered and the processor is operational.

Care should be taken to prevent Intel® Xeon® Processor D-1500 Product Family from driving an active '1' on a pin sharing the serial LED capability. Since the SIO could be driving the line to 0, having Intel® Xeon® Processor D-1500 Product Family drive a 1 would create a high current path. A recommendation to avoid this condition involves choosing a GPIO defaulting to an input. The GP_SER_BLINK register should be set first before changing the direction of the pin to an output. This sequence ensures the open-drain capability of the buffer is properly configured before enabling the pin as an output.

3.14.5.2 Serial Message Format

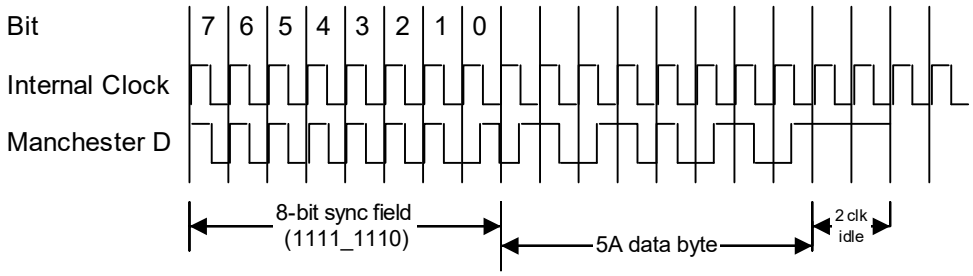
In order to serialize the data onto the GPIO, an initial state of high-Z is assumed. The SIO is required to have its LED control pin in a high-Z state as well to allow Intel® Xeon® Processor D-1500 Product Family to blink the LED (refer to the reference diagram).

The three components of the serial message include the sync, data, and idle fields. The sync field is 7 bits of '1' data followed by 1 bit of '0' data. Starting from the high-Z state (LED on) provides external hardware a known initial condition and a known pattern. In case one or more of the leading 1 sync bits are lost, the 1s followed by 0 provide a clear indication of 'end of sync'. This pattern will be used to 'lock' external sampling logic to the encoded clock.

The data field is shifted out with the highest byte first (MSB). Within each byte, the most significant bit is shifted first (MSb).

The idle field is enforced by the hardware and is at least 2 bit times long. The hardware will not clear the Busy and Go bits until this idle time is met. Supporting the idle time in hardware prevents time-based counting in BIOS as the hardware is immediately ready for the next serial code when the Go bit is cleared. The idle state is represented as a high-Z condition on the pin. If the last transmitted bit is a 1, returning to the idle state will result in a final 0-1 transition on the output Manchester data. Two full bit times of idle correspond to a count of 4 time intervals (the width of the time interval is controlled by the DRS field).

The following waveform shows a 1-byte serial write with a data byte of 5Ah. The internal clock and bit position are for reference purposes only. The Manchester D is the resultant data generated and serialized onto the GPIO. Since the buffer is operating in open-drain mode the transitions are from high-Z to 0 and back.



3.15 SATA Host Controller (D31:F2, F5)

The SATA function in Intel® Xeon® Processor D-1500 Product Family has three modes of operation to support different operating system conditions. In the case of Native IDE enabled operating systems, Intel® Xeon® Processor D-1500 Product Family uses two controllers to enable all six ports of the bus. The first controller (Device 31: Function 2) supports ports 0 – 3 and the second controller (Device 31: Function 5) supports ports 4 and 5. When using a legacy operating system, only one controller (Device 31: Function 2) is available that supports ports 0 – 3. In AHCI or RAID mode, only one controller (Device 31: Function 2) is utilized enabling all six ports and the second controller (Device 31: Function 5) shall be disabled.

The MAP register, Section 9.1.27, provides the ability to share PCI functions. When sharing is enabled, all decode of I/O is done through the SATA registers. Device 31, Function 1 (IDE controller) is hidden by software writing to the Function Disable Register (D31, F0, Offset F2h, bit 1), and its configuration registers are not used.

Intel® Xeon® Processor D-1500 Product Family SATA controllers feature six sets of interface signals (ports) that can be independently enabled or disabled (they cannot be tri-stated or driven low). Each interface is supported by an independent DMA controller.

Intel® Xeon® Processor D-1500 Product Family SATA controllers interact with an attached mass storage device through a register interface that is equivalent to that presented by a traditional IDE host adapter. The host software follows existing standards and conventions when accessing the register interface and follows standard command protocol conventions.

Note: SATA interface transfer rates are independent of UDMA mode settings. SATA interface transfer rates will operate at the bus's maximum speed, regardless of the UDMA mode reported by the SATA device or the system BIOS.

3.15.1 SATA 6 Gb/s Support

Intel® Xeon® Processor D-1500 Product Family supports SATA 6 Gb/s transfers with all capable SATA devices.

3.15.2 SATA Feature Support

Feature	Intel® Xeon® Processor D-1500 Product Family (AHCI/RAID Disabled)	Intel® Xeon® Processor D-1500 Product Family (AHCI/RAID Enabled)
Native Command Queuing (NCQ)	N/A	Supported
Auto Activate for DMA	N/A	Supported
Hot-Plug Support	N/A	Supported
Asynchronous Signal Recovery	N/A	Supported
6 Gb/s Transfer Rate	Supported	Supported
ATAPI Asynchronous Notification	N/A	Supported
Host & Link Initiated Power Management	N/A	Supported
Staggered Spin-Up	Supported	Supported
Command Completion Coalescing	N/A	N/A
External SATA	N/A	Supported

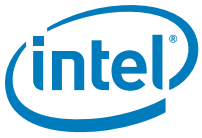
Feature	Description
Native Command Queuing (NCQ)	Allows the device to reorder commands for more efficient data transfers
Auto Activate for DMA	Collapses a DMA Setup then DMA Activate sequence into a DMA Setup only
Hot-Plug Support	Allows for device detection without power being applied and ability to connect and disconnect devices without prior notification to the system
Asynchronous Signal Recovery	Provides a recovery from a loss of signal or establishing communication after Hot-Plug
6 Gb/s Transfer Rate	Capable of data transfers up to 6 Gb/s
ATAPI Asynchronous Notification	A mechanism for a device to send a notification to the host that the device requires attention
Host & Link Initiated Power Management	Capability for the host controller or device to request Partial and Slumber interface power states
Staggered Spin-Up	Enables the host the ability to spin up hard drives sequentially to prevent power load problems on boot
Command Completion Coalescing	Reduces interrupt and completion overhead by allowing a specified number of commands to complete and then generating an interrupt to process the commands

3.15.3 Theory of Operation

3.15.3.1 Standard ATA Emulation

Intel® Xeon® Processor D-1500 Product Family contains a set of registers that shadow the contents of the legacy IDE registers. The behavior of the Command and Control Block registers, PIO, and DMA data transfers, resets, and interrupts are all emulated.

Note: Intel® Xeon® Processor D-1500 Product Family will assert INTR when the master device completes the EDD command regardless of the command completion status of the slave device. If the master completes EDD first, an INTR is generated and BSY will remain '1' until the slave completes the command. If the slave completes EDD first, BSY will be '0' when the master completes the EDD command and asserts INTR. Software must wait for busy to clear (0) before completing an EDD command, as required by the ATA5 through ATA7 (T13) industry standards.



3.15.3.2 48-Bit LBA Operation

The SATA host controller supports 48-bit LBA through the host-to-device register FIS when accesses are performed using writes to the task file. The SATA host controller will ensure that the correct data is put into the correct byte of the host-to-device FIS.

There are special considerations when reading from the task file to support 48-bit LBA operation. Software may need to read all 16-bits. Since the registers are only 8-bits wide and act as a FIFO, a bit must be set in the device/control register, which is at offset 3F6h for primary and 376h for secondary (or their native counterparts).

If software clears Bit 7 of the control register before performing a read, the last item written will be returned from the FIFO. If software sets Bit 7 of the control register before performing a read, the first item written will be returned from the FIFO.

3.15.4 SATA Swap Bay Support

Intel® Xeon® Processor D-1500 Product Family provides for basic SATA swap bay support using the PSC register configuration bits and power management flows. A device can be powered down by software and the port can then be disabled, allowing removal and insertion of a new device.

Note: This SATA swap bay operation requires board hardware (implementation specific), BIOS, and operating system support.

3.15.5 Hot-Plug Operation

Intel® Xeon® Processor D-1500 Product Family supports Hot-Plug Surprise removal and Insertion Notification. An internal SATA port with a Mechanical Presence Switch can support PARTIAL and SLUMBER with Hot-Plug Enabled. Software can take advantage of power savings in the low power states while enabling Hot-Plug operation. See Chapter 7 of the AHCI specification for details.

3.15.6 Function Level Reset Support (FLR)

The SATA Host Controller supports the Function Level Reset (FLR) capability. The FLR capability can be used in conjunction with Intel Virtualization Technology. FLR allows an operating system in a Virtual Machine to have complete control over a device, including its initialization, without interfering with the rest of the platform. The device provides a software interface that enables the Operating System to reset the whole device as if a platform reset was asserted.

3.15.6.1 FLR Steps

3.15.6.1.1 FLR Initialization

1. A FLR is initiated by software writing a ‘1’ to the Initiate FLR bit.
2. All subsequent requests targeting the Function will not be claimed and will be Master Abort Immediate on the bus. This includes any configuration, I/O or Memory cycles, however, the Function shall continue to accept completions targeting the Function.

3.15.6.1.2 FLR Operation

The Function will Reset all configuration, I/O and memory registers of the Function except those indicated otherwise and reset all internal states of the Function to the default or initial condition.

3.15.6.1.3 FLR Completion

The Initiate FLR bit is reset (cleared) when the FLR reset is completed. This bit can be used to indicate to the software that the FLR reset is completed.

Note: From the time Initiate FLR bit is written to 1 software must wait at least 100 ms before accessing the function.

3.15.7 Power Management Operation

Power management of Intel® Xeon® Processor D-1500 Product Family SATA controller and ports will cover operations of the host controller and the SATA wire.

3.15.7.1 Power State Mappings

The D0 PCI power management state for device is supported by Intel® Xeon® Processor D-1500 Product Family SATA controller.

SATA devices may also have multiple power states. From parallel ATA, three device states are supported through ACPI. They are:

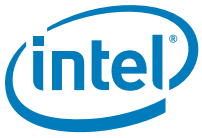
- D0 – Device is working and instantly available.
- D1 – Device enters when it receives a STANdBY IMMEDIATE command. Exit latency from this state is in seconds
- D3 – From the SATA device's perspective, no different than a D1 state, in that it is entered using the STANdBY IMMEDIATE command. However, an ACPI method is also called which will reset the device and then cut its power.

Each of these device states are subsets of the host controller's D0 state.

Finally, SATA defines three PHY layer power states, which have no equivalent mappings to parallel ATA. They are:

- PHY READY – PHY logic and PLL are both on and active
- Partial – PHY logic is powered, but in a reduced state. Exit latency is no longer than 10 ns
- Slumber – PHY logic is powered, but in a reduced state. Exit latency can be up to 10 ms.

Since these states have much lower exit latency than the ACPI D1 and D3 states, the SATA controller defines these states as sub-states of the device D0 state.



3.15.7.2 Power State Transitions

3.15.7.2.1 Partial and Slumber State Entry/Exit

The partial and slumber states save interface power when the interface is idle. It would be most analogous to CLKRUN# (in power savings, not in mechanism), where the interface can have power saved while no commands are pending. The SATA controller defines PHY layer power management (as performed using primitives) as a driver operation from the host side, and a device proprietary mechanism on the device side. The SATA controller accepts device transition types, but does not issue any transitions as a host. All received requests from a SATA device will be ACKed.

When an operation is performed to the SATA controller such that it needs to use the SATA cable, the controller must check whether the link is in the Partial or Slumber states, and if so, must issue a COM_WAKE to bring the link back online. Similarly, the SATA device must perform the same action.

3.15.7.2.2 Device D1, D3 States

These states are entered after some period of time when software has determined that no commands will be sent to this device for some time. The mechanism for putting a device in these states does not involve any work on the host controller, other then sending commands over the interface to the device. The command most likely to be used in ATA/ATAPI is the "STANdBY IMMEDIATE" command.

3.15.7.2.3 Host Controller $D3_{HOT}$ State

After the interface and device have been put into a low power state, the SATA host controller may be put into a low power state. This is performed using the PCI power management registers in configuration space. There are two very important aspects to note when using PCI power management.

1. When the power state is D3, only accesses to configuration space are allowed. Any attempt to access the memory or I/O spaces will result in master abort.
2. When the power state is D3, no interrupts may be generated, even if they are enabled. If an interrupt status bit is pending when the controller transitions to D0, an interrupt may be generated.

When the controller is put into D3, it is assumed that software has properly shut down the device and disabled the ports. Therefore, there is no need to sustain any values on the port wires. The interface will be treated as if no device is present on the cable, and power will be minimized.

When returning from a D3 state, an internal reset will not be performed.

3.15.7.2.4 Non-AHCI Mode PME# Generation

When in non-AHCI mode (legacy mode) of operation, the SATA controller does not generate PME#. This includes attach events (since the port must be disabled), or interlock switch events (using the SATAGP pins).

3.15.7.3 SMI Trapping (APM)

D31:F2:Offset C0h (see Section 8.1.43) contain control for generating SMI# on accesses to the IDE I/O spaces. These bits map to the legacy ranges (1F0–1F7h, 3F6h, 170–177h, and 376h) and native IDE ranges defined by PCMdBA, PCTLBA, SCMdBA an SCTLBA. If the SATA controller is in legacy mode and is using these addresses,

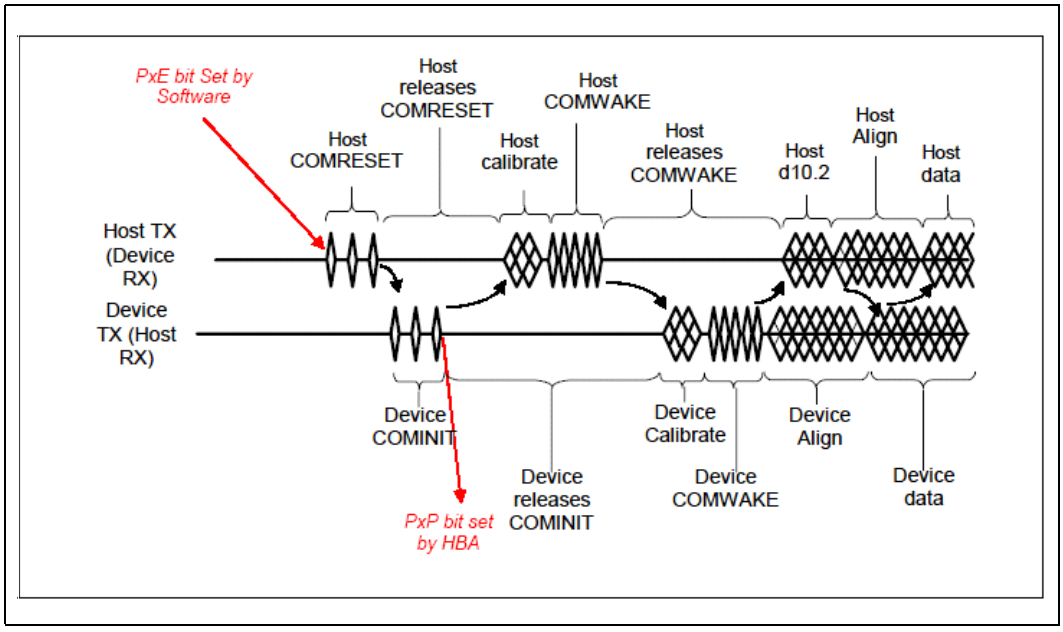
accesses to one of these ranges with the appropriate bit set causes the cycle to not be forwarded to the SATA controller, and for an SMI# to be generated. If an access to the Bus-Master IDE registers occurs while trapping is enabled for the device being accessed, then the register is updated, an SMI# is generated, and the device activity status bits (Section 8.1.44) are updated indicating that a trap occurred.

3.15.8 SATA Device Presence

In legacy mode, the SATA controller does not generate interrupts based on Hot-Plug/ unplug events. However, the SATA PHY does know when a device is connected (if not in a partial or slumber state), and it s beneficial to communicate this information to host software as this will greatly reduce boot times and resume times.

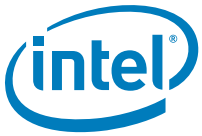
The flow used to indicate SATA device presence is shown in Figure 3-8. The 'PxE' bit refers to PCS.P[3:0]E bits, depending on the port being checked and the 'PxP' bits refer to the PCS.P[3:0]P bits, depending on the port being checked. If the PCS/PxP bit is set a device is present, if the bit is cleared a device is not present. If a port is disabled, software can check to see if a new device is connected by periodically re-enabling the port and observing if a device is present, if a device is not present it can disable the port and check again later. If a port remains enabled, software can periodically poll PCS.PxP to see if a new device is connected.

Figure 3-8. Flow for Port Enable / Device Present Bits



3.15.9 SATA LED

The SATALED# output is driven whenever the BSY bit is set in any SATA port. The SATALED# is an active-low open-drain output. When SATALED# is low, the LED should be active. When SATALED# is high, the LED should be inactive.



3.15.10 AHCI Operation

Intel® Xeon® Processor D-1500 Product Family provides hardware support for Advanced Host Controller Interface (AHCI), a programming interface for SATA host controllers developed through a joint industry effort. AHCI defines transactions between the SATA controller and software and enables advanced performance and usability with SATA. Platforms supporting AHCI may take advantage of performance features such as no master/slave designation for SATA devices—each device is treated as a master—and hardware assisted native command queuing. AHCI also provides usability enhancements such as Hot-Plug. AHCI requires appropriate software support (such as, an AHCI driver) and for some features, hardware support in the SATA device or additional platform hardware.

Intel® Xeon® Processor D-1500 Product Family supports all of the mandatory features of the *Serial ATA Advanced Host Controller Interface Specification*, Revision 1.3 and many optional features, such as hardware assisted native command queuing, aggressive power management, LED indicator support, and Hot-Plug through the use of interlock switch support (additional platform hardware and software may be required depending upon the implementation).

Note: For reliable device removal notification while in AHCI operation without the use of interlock switches (surprise removal), interface power management should be disabled for the associated port. See Section 7.3.1 of the *AHCI Specification* for more information.

3.15.11 SGPIO Signals

The SGPIO signals, in accordance to the SFF-8485 specification, support per-port LED signaling. These signals are not related to SATALED#, which allows for simplified indication of SATA command activity. The SGPIO group interfaces with an external controller chip that fetches and serializes the data for driving across the SGPIO bus. The output signals then control the LEDs. This feature is only valid in AHCI/RAID mode.

Note: Intel does not validate all possible usage cases of this feature. Customers should validate their specific design implementation on their own platforms.

3.15.11.1 Mechanism

The enclosure management for SATA Controller 1 (Device 31: Function 2) involves sending messages that control LEDs in the enclosure. The messages for this function are stored after the normal registers in the AHCI BAR, at Offset 580h bytes for Intel® Xeon® Processor D-1500 Product Family from the beginning of the AHCI BAR as specified by the EM_LOC global register (Section 8.4.1.6).

Software creates messages for transmission in the enclosure management message buffer. The data in the message buffer should not be changed if CTL.TM bit is set by software to transmit an update message. Software should only update the message buffer when CTL.TM bit is cleared by hardware otherwise the message transmitted will be indeterminate. Software then writes a register to cause hardware to transmit the message or take appropriate action based on the message content. The software should only create message types supported by the controller, which is LED messages for Intel® Xeon® Processor D-1500 Product Family. If the software creates other non LED message types (such as, SAF-TE, SES-2), the SGPIO interface may hang and the result is indeterminate.

During reset all SGPIO pins will be in tri-state state. The interface will continue staying in tri-state state after reset until the first transmission occurs, when software programs the message buffer and sets the transmit bit CTL.TM. The SATA host controller will initiate the transmission by driving SCLOCK and at the same time driving the SLOAD to "0" prior to the actual bit stream transmission. The Host will drive SLOAD low for at least 5 SCLOCK then only start the bit stream by driving the SLOAD to high. SLOAD will be driven high for 1 SCLOCK, followed by vendor-specific pattern that is default to "0000" if software is yet to program the value. A total of 18-bit streams from 6 ports (Port0, Port1, Port2, Port3, Port4 and Port5) of 3-bit per port LED message will be transmitted on SDATAOUT0 pin after the SLOAD is driven high for 1 SCLOCK. Only 2 ports (port4, and port 5) of 6-bit total LED message follow by 12 bits of tri-state value will be transmitted out on SDATAOUT1 pin.

All the default LED message values will be high prior to software setting them, except the Activity LED message that is configured to be hardware driven that will be generated based on the activity from the respective port. All the LED message values will be driven to '1' for the port that is unimplemented as indicated in the Port Implemented register regardless of the software programmed value through the message buffer.

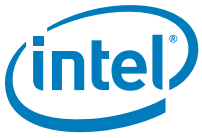
There are 2 different ways of resetting Intel® Xeon® Processor D-1500 Product Family's SGPIO interface, asynchronous reset and synchronous reset. Asynchronous reset is caused by platform reset to cause the SGPIO interface to be tri-state asynchronously. Synchronous reset is caused by setting the CTL.RESET bit, clearing the GHC.AE bit or HBA reset, where Host Controller will complete the existing full bit stream transmission then only tri-state all the SGPIO pins. After the reset, both synchronous and asynchronous, the SGPIO pins will stay tri-stated.

Note: Intel® Xeon® Processor D-1500 Product Family Host Controller does not ensure that it will cause the target SGPIO device or controller to be reset. Software is responsible to keep Intel® Xeon® Processor D-1500 Product Family SGPIO interface in tri-state for 2 second to cause a reset on the target of the SGPIO interface.

3.15.11.2 Message Format

Messages shall be constructed with a one DWord header that describes the message to be sent followed by the actual message contents. The first DWord shall be constructed as follows:

Bit	Description
31:28	Reserved
27:24	**Message Type (MTYPE):** Specifies the type of the message. The message types are: 0h = LED 1h = SAF-TE 2h = SES-2 3h = SGPIO (register based interface) All other values reserved
23:16	**Data Size (DSIZE):** Specifies the data size in bytes. If the message (enclosure services command) has a data buffer that is associated with it that is transferred, the size of that data buffer is specified in this field. If there is no separate data buffer, this field shall have a value of '0'. The data directly follows the message in the message buffer. For Intel® Xeon® Processor D-1500 Product Family, this value should always be '0'.
15:8	**Message Size (MSIZE):** Specifies the size of the message in bytes. The message size does not include the one DWord header. A value of '0' is invalid. For Intel® Xeon® Processor D-1500 Product Family, the message size is always 4 bytes.



Bit	Description
7:0	Reserved

The SAF-TE, SES-2, and SGPIO message formats are defined in the corresponding specifications, respectively. The LED message type is defined in Section 3.15.11.3. It is the responsibility of software to ensure the content of the message format is correct. If the message type is not programmed as 'LED' for this controller, the controller shall not take any action to update its LEDs. For LED message type, the message size always consists of 4 bytes.

3.15.11.3 LED Message Type

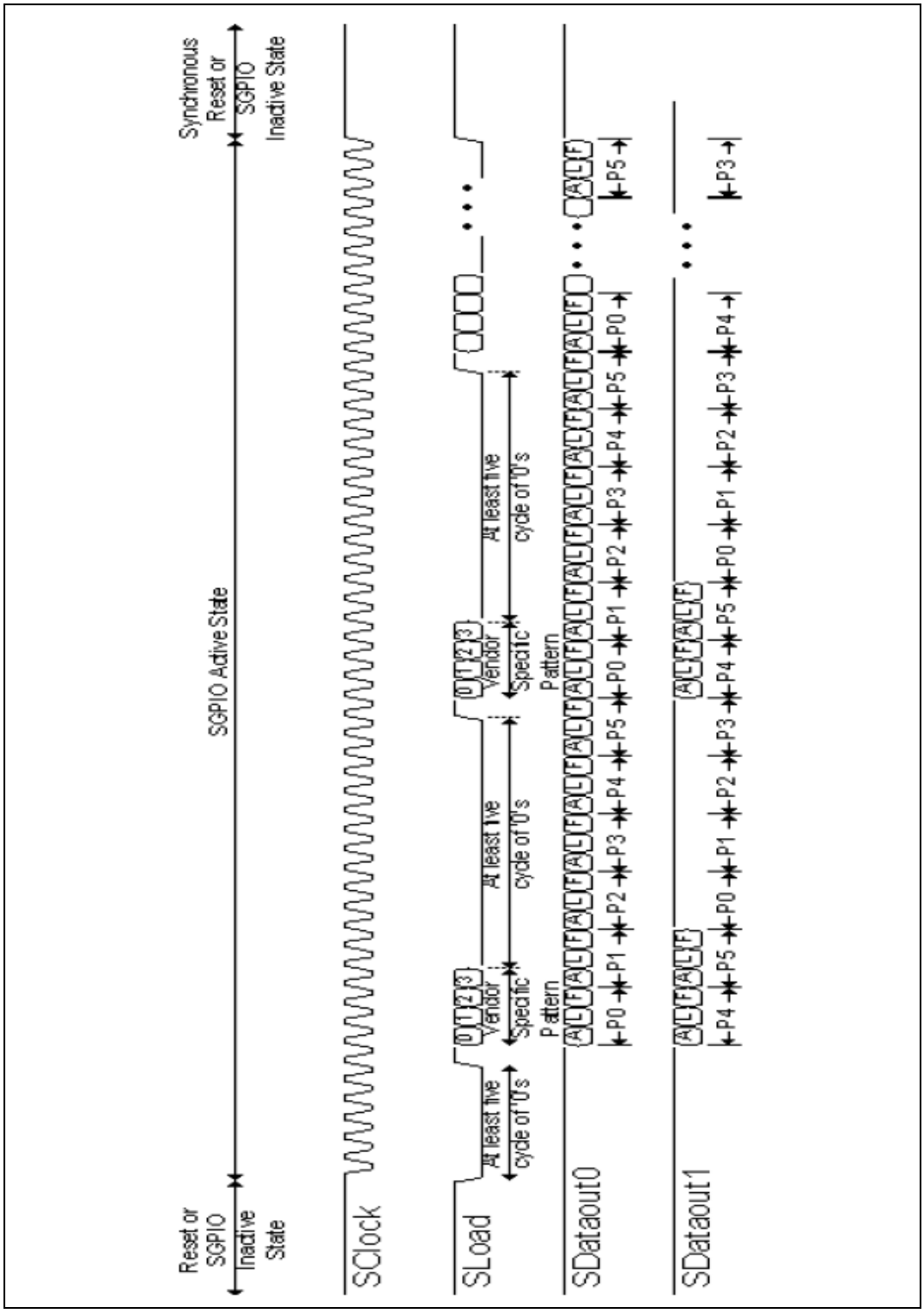
The LED message type specifies the status of up to three LEDs. Typically, the usage for these LEDs is activity, fault, and locate. Not all implementations necessarily contain all LEDs (for example, some implementations may not have a locate LED). The message identifies the HBA port number and the Port Multiplier port number that the slot status applies to. If a Port Multiplier is not in use with a particular device, the Port Multiplier port number shall be '0'. The format of the LED message type is defined in Table 3-37. The LEDs shall retain their values until there is a following update for that particular slot.

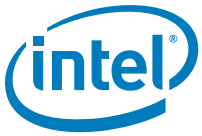
Table 3-37. Multi-activity LED Message Type

Byte	Description
3-2	**Value (VAL):** This field describes the state of each LED for a particular location. There are three LEDs that may be supported by the HBA. Each LED has 3 bits of control. **LED values are:** 000b – LED shall be off 001b – LED shall be solid on as perceived by human eye All other values reserved **The LED bit locations are:** Bits 2:0 – Activity LED (may be driven by hardware) Bits 5:3 – Vendor Specific LED (such as locate) Bits 8:6 - Vendor Specific LED (such as fault) Bits 15:9 – Reserved **Vendor specific message is:** Bit 3:0 – Vendor Specific Pattern Bit 15:4 – Reserved ***Note:*** If Activity LED Hardware Driven (ATTR.ALHD) bit is set, host will output the hardware LED value sampled internally and will ignore software written activity value on bit [2:0]. Since Intel® Xeon® Processor D-1500 Product Family Enclosure Management does not support port multiplier based LED message, the LED message will be generated independently based on respective port's operation activity. Vendor specific LED values Locate (Bits 5:3) and Fault (Bits 8:6) always are driven by software.
1	**Port Multiplier Information:** Specifies slot specific information related to Port Multiplier. Bits 3:0 specify the Port Multiplier port number for the slot that requires the status update. If a Port Multiplier is not attached to the device in the affected slot, the Port Multiplier port number shall be '0'. Bits 7:4 are reserved. Intel® Xeon® Processor D-1500 Product Family does not support LED messages for devices behind a Port Multiplier. This byte should be 0.
0	**HBA Information:** Specifies slot specific information related to the HBA. Bits 4:0 – HBA port number for the slot that requires the status update. Bit 5 – If set to '1', value is a vendor specific message that applies to the entire enclosure. If cleared to '0', value applies to the port specified in bits 4:0. Bits 7:6 – Reserved

3.15.11.4 SGPIO Waveform

Figure 3-9. Serial Data transmitted over the SGPIO Interface





3.16 High Precision Event Timers (HPET)

This function provides a set of timers that can be used by the operating system. The timers are defined such that the operating system may be able to assign specific timers to be used directly by specific applications. Each timer can be configured to cause a separate interrupt.

Intel® Xeon® Processor D-1500 Product Family provides eight timers. The timers are implemented as a single counter, and each timer has its own comparator and value register. The counter increases monotonically. Each individual timer can generate an interrupt when the value in its value register matches the value in the main counter.

The registers associated with these timers are mapped to a memory space (much like the I/O APIC). However, it is not implemented as a standard PCI function. The BIOS reports to the operating system the location of the register space. The hardware can support an assignable decode space; however, the BIOS sets this space prior to handing it over to the operating system. It is not expected that the operating system will move the location of these timers once it is set by the BIOS.

3.16.1 Timer Accuracy

The timers are accurate over any 1 ms period to within 0.05% of the time specified in the timer resolution fields.

Within any 100 microsecond period, the timer reports a time that is up to two ticks too early or too late. Each tick is less than or equal to 100 ns, so this represents an error of less than 0.2%.

The timer is monotonic. It does not return the same value on two consecutive reads (unless the counter has rolled over and reached the same value).

The main counter is clocked by the 14.31818 MHz clock. The accuracy of the main counter is as accurate as the 14.31818 MHz clock.

3.16.2 Interrupt Mapping

Mapping Option #1 (Legacy Replacement Option)

In this case, the Legacy Replacement Rout bit (LEG_RT_CNF) is set. This forces the mapping found in Table 3-38.

Table 3-38. Legacy Replacement Routing

Timer	8259 Mapping	APIC Mapping	Comment
0	IRQ0	IRQ2	In this case, the 8254 timer will not cause any interrupts
1	IRQ8	IRQ8	In this case, the RTC will not cause any interrupts.
2 & 3	Per IRQ Routing Field.	Per IRQ Routing Field	
4, 5, 6, 7	**not available**	**not available**	

Note: The Legacy Option does not preclude delivery of IRQ0/IRQ8 using processor interrupts messages.

Mapping Option #2 (Standard Option)

In this case, the Legacy Replacement Rout bit (LEG_RT_CNF) is 0. Each timer has its own routing control. The interrupts can be routed to various interrupts in the 8259 or I/O APIC. A capabilities field indicates which interrupts are valid options for routing. If a timer is set for edge-triggered mode, the timers should not be shared with any legacy interrupts.

For Intel® Xeon® Processor D-1500 Product Family, the only supported interrupt values are as follows:

Timer 0 and 1: IRQ20, 21, 22 & 23 (I/O APIC only).

Timer 2: IRQ11 (8259 or I/O APIC) and IRQ20, 21, 22 & 23 (I/O APIC only).

Timer 3: IRQ12 (8259 or I/O APIC) and IRQ 20, 21, 22 & 23 (I/O APIC only).

Interrupts from Timer 4, 5, 6, 7 can only be delivered using processor message interrupts.

Mapping Option #3 (Processor Message Option)

In this case, the interrupts are mapped directly to processor messages without going to the 8259 or I/O (x) APIC. To use this mode, the interrupt must be configured to edge-triggered mode. The Tn_PROCMSG_EN_CNF bit must be set to enable this mode.

When the interrupt is delivered to the processor, the message is delivered to the address indicated in the Tn_PROCMSG_INT_ADDR field. The data value for the write cycle is specified in the Tn_PROCMSG_INT_VAL field.

Notes:

1. The processor message interrupt delivery option has HIGHER priority and is mutually exclusive to the standard interrupt delivery option. Thus, if the Tn_PROCMSG_EN_CNF bit is set, the interrupts will be delivered directly to the processor, rather than using the APIC or 8259.

The processor message interrupt delivery can be used even when the legacy mapping is used.

3.16.3 Periodic versus Non-Periodic Modes

Non-Periodic Mode

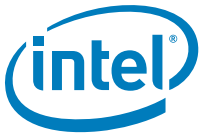
Timer 0 is configurable to 32 (default) or 64-bit mode, whereas Timers 1:7 only support 32-bit mode (See Section 14.1.5).

All of the timers support non-periodic mode.

Refer to Section 2.3.9.2.1 of the *IA-PC HPET Specification* for a description of this mode.

Periodic Mode

Timer 0 is the only timer that supports periodic mode. Refer to Section 2.3.9.2.2 of the *IA-PC HPET Specification* for a description of this mode.



The following usage model is expected:

1. Software clears the ENABLE_CNF bit to prevent any interrupts.
2. Software Clears the main counter by writing a value of 00h to it.
3. Software sets the TIMER0_VAL_SET_CNF bit.
4. Software writes the new value in the TIMER0_COMPARATOR_VAL register.
5. Software sets the ENABLE_CNF bit to enable interrupts.

The Timer 0 Comparator Value register cannot be programmed reliably by a single 64-bit write in a 32-bit environment except if only the periodic rate is being changed during run-time. If the actual Timer 0 Comparator Value needs to be reinitialized, then the following software solution will always work regardless of the environment:

1. Set TIMER0_VAL_SET_CNF bit.
2. Set the lower 32 bits of the Timer0 Comparator Value register.
3. Set TIMER0_VAL_SET_CNF bit.
4. Set the upper 32 bits of the Timer0 Comparator Value register.

3.16.4 Enabling the Timers

The BIOS or operating system PnP code should route the interrupts. This includes the Legacy Rout bit, Interrupt Rout bit (for each timer), interrupt type (to select the edge or level type for each timer)

The Device Driver code should do the following for an available timer:

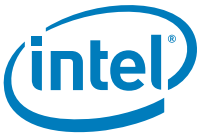
1. Set the Overall Enable bit (Offset 10h, bit 0).
2. Set the timer type field (selects one-shot or periodic).
3. Set the interrupt enable.
4. Set the comparator value.

3.16.5 Interrupt Levels

Interrupts directed to the internal 8259s are active high. See Section 3.9 for information regarding the polarity programming of the I/O APIC for detecting internal interrupts.

If the interrupts are mapped to the 8259 or I/O APIC and set for level-triggered mode, they can be shared with legacy interrupts. They may be shared although it is unlikely for the operating system to attempt to do this.

If more than one timer is configured to share the same IRQ (using the TIMERn_INT_ROUT_CNF fields), then the software must configure the timers to level-triggered mode. Edge-triggered interrupts cannot be shared.



3.16.6 Handling Interrupts

If each timer has a unique interrupt and the timer has been configured for edge-triggered mode, then there are no specific steps required. No read is required to process the interrupt.

If a timer has been configured to level-triggered mode, then its interrupt must be cleared by the software. This is done by reading the interrupt status register and writing a 1 back to the bit position for the interrupt to be cleared.

Independent of the mode, software can read the value in the main counter to see how much time has passed between when the interrupt was generated and when it was first serviced.

If Timer 0 is set up to generate a periodic interrupt, the software can check to see how much time remains until the next interrupt by checking the timer value register.

3.16.7 Issues Related to 64-Bit Timers with 32-Bit Processors

A 32-bit timer can be read directly using processors that are capable of 32-bit or 64-bit instructions. However, a 32-bit processor may not be able to directly read 64-bit timer. A race condition comes up if a 32-bit processor reads the 64-bit register using two separate 32-bit reads. The danger is that just after reading one half, the other half rolls over and changes the first half.

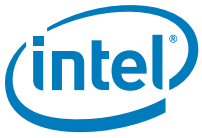
If a 32-bit processor needs to access a 64-bit timer, it must first halt the timer before reading both the upper and lower 32-bits of the timer. If a 32-bit processor does not want to halt the timer, it can use the 64-bit timer as a 32-bit timer by setting the TIMERn_32MODE_CNF bit. This causes the timer to behave as a 32-bit timer. The upper 32-bits are always 0.

Alternatively, software may do a multiple read of the counter while it is running. Software can read the high 32 bits, then the low 32 bits, the high 32 bits again. If the high 32 bits have not changed between the two reads, then a rollover has not happened and the low 32 bits are valid. If the high 32 bits have changed between reads, then the multiple reads are repeated until a valid read is performed.

Note: On a 64-bit platform, if software attempts a 64 bit read of the 64-bit counter, software must be aware that some platforms may split the 64 bit read into two 32 bit reads. The read maybe inaccurate if the low 32 bits roll over between the high and low reads.

3.17 USB EHCI Host Controllers (D29:F0)

Intel® Xeon® Processor D-1500 Product Family contains one Enhanced Host Controller Interface (EHCI) host controllers which support up to four USB 2.0 high-speed root ports. USB 2.0 allows data transfers up to 480 Mb/s. USB 2.0 based Debug Port is also implemented in Intel® Xeon® Processor D-1500 Product Family.



3.17.1 EHC Initialization

The following descriptions step through the expected Intel® Xeon® Processor D-1500 Product Family Enhanced Host Controller (EHC) initialization sequence in chronological order, beginning with a complete power cycle in which the suspend well and core well have been off.

3.17.1.1 BIOS Initialization

BIOS performs a number of platform customization steps after the core well has powered up. Contact your Intel Field Representative for additional Intel® Xeon® Processor D-1500 Product Family BIOS information.

3.17.1.2 Driver Initialization

See Chapter 4 of the *Enhanced Host Controller Interface Specification for Universal Serial Bus,* Revision 1.0.

3.17.1.3 EHC Resets

In addition to the standard Intel® Xeon® Processor D-1500 Product Family hardware resets, portions of the EHC are reset by the HCRESET bit and the transition from the $D3_{HOT}$ device power management state to the D0 state. The effects of each of these resets are:

Reset	Does Reset	Does Not Reset	Comments
HCRESET bit set.	Memory space registers except Structural Parameters (which is written by BIOS).	Configuration registers.	The HCRESET must only affect registers that the EHCI driver controls. PCI Configuration space and BIOS-programmed parameters cannot be reset.
Software writes the Device Power State from $D3_{HOT}$ (11b) to D0 (00b).	Core well registers (except BIOS-programmed registers).	Suspend well registers; BIOS-programmed core well registers.	The D3-to-D0 transition must not cause wake information (suspend well) to be lost. It also must not clear BIOS-programmed registers because BIOS may not be invoked following the D3-to-D0 transition.

If the detailed register descriptions give exceptions to these rules, those exceptions override these rules. This summary is provided to help explain the reasons for the reset policies.

3.17.2 Data Structures in Main Memory

See Section 3 and Appendix B of the *Enhanced Host Controller Interface Specification for Universal Serial Bus,* Revision 1.0 for details.

3.17.3 USB 2.0 Enhanced Host Controller DMA

Intel® Xeon® Processor D-1500 Product Family USB 2.0 EHC implements three sources of USB packets. They are, in order of priority on USB during each microframe:

1. The USB 2.0 Debug Port,
2. The Periodic DMA engine, and
3. The Asynchronous DMA engine.

Intel® Xeon® Processor D-1500 Product Family always performs any currently-pending debug port transaction at the beginning of a microframe, followed by any pending periodic traffic for the current microframe. If there is time left in the microframe, then the EHC performs any pending asynchronous traffic until the end of the microframe (EOF1). The debug port traffic is only presented on Port 1 and Port 9, while the other ports are idle during this time.

3.17.4 Data Encoding and Bit Stuffing

See Chapter 8 of the *Universal Serial Bus Specification, Revision 2.0.*

3.17.5 Packet Formats

See Chapter 8 of the *Universal Serial Bus Specification, Revision 2.0*.

Intel® Xeon® Processor D-1500 Product Family EHCI allows entrance to USB test modes, as defined in the USB 2.0 specification, including Test J, Test Packet, and so on. However, Intel® Xeon® Processor D-1500 Product Family Test Packet test mode interpacket gap timing may not meet the USB 2.0 specification.

3.17.6 USB 2.0 Interrupts and Error Conditions

Section 4 of the *Enhanced Host Controller Interface Specification for Universal Serial Bus,* Revision 1.0 goes into detail on the EHC interrupts and the error conditions that cause them. All error conditions that the EHC detects can be reported through the EHCI Interrupt status bits. Only Intel® Xeon® Processor D-1500 Product Family-specific interrupt and error-reporting behavior is documented in this section. The EHCI Interrupts section must be read first, followed by this section of the datasheet to fully comprehend the EHC interrupt and error-reporting functionality.

- Based on the EHC Buffer sizes and buffer management policies, the Data Buffer Error can never occur on Intel® Xeon® Processor D-1500 Product Family.
- Master Abort and Target Abort responses from hub interface on EHC-initiated read packets will be treated as Fatal Host Errors. The EHC halts when these conditions are encountered.
- Intel® Xeon® Processor D-1500 Product Family may assert the interrupts which are based on the interrupt threshold as soon as the status for the last complete transaction in the interrupt interval has been posted in the internal write buffers. The requirement in the *Enhanced Host Controller Interface Specification for Universal Serial Bus,* Revision 1.0 (that the status is written to memory) is met internally.
- Since Intel® Xeon® Processor D-1500 Product Family supports the 1024-element Frame List size, the Frame List Rollover interrupt occurs every 1024 milliseconds.
- Intel® Xeon® Processor D-1500 Product Family delivers interrupts using PIRQH#.
- Intel® Xeon® Processor D-1500 Product Family does not modify the CERR count on an Interrupt IN when the “Do Complete-Split” execution criteria are not met.
- For complete-split transactions in the Periodic list, the “Missed Microframe” bit does not get set on a control-structure-fetch that fails the late-start test. If subsequent

accesses to that control structure do not fail the late-start test, then the "Missed Microframe" bit will get set and written back.

3.17.6.1 Aborts on USB 2.0-Initiated Memory Reads

If a read initiated by the EHC is aborted, the EHC treats it as a fatal host error. The following actions are taken when this occurs:

- The Host System Error status bit is set.
- The DMA engines are halted after completing up to one more transaction on the USB interface.
- If enabled (by the Host System Error Enable), then an interrupt is generated.
- If the status is Master Abort, then the Received Master Abort bit in configuration space is set.
- If the status is Target Abort, then the Received Target Abort bit in configuration space is set.
- If enabled (by the SERR Enable bit in the function's configuration space), then the Signaled System Error bit in configuration bit is set.

3.17.7 USB 2.0 Power Management

3.17.7.1 Pause Feature

This feature allows platforms to dynamically enter low-power states during brief periods when the system is idle (that is, between keystrokes). This is useful for enabling power management features in Intel® Xeon® Processor D-1500 Product Family. The policies for entering these states typically are based on the recent history of system bus activity to incrementally enter deeper power management states. Normally, when the EHC is enabled, it regularly accesses main memory while traversing the DMA schedules looking for work to do; this activity is viewed by the power management software as a non-idle system, thus preventing the power managed states to be entered. Suspending all of the enabled ports can prevent the memory accesses from occurring, but there is an inherent latency overhead with entering and exiting the suspended state on the USB ports that makes this unacceptable for the purpose of dynamic power management. As a result, the EHCI software drivers are allowed to pause the EHC DMA engines when it knows that the traffic patterns of the attached devices can afford the delay. The pause only prevents the EHC from generating memory accesses; the SOF packets continue to be generated on the USB ports (unlike the suspended state).

3.17.7.2 Suspend Feature

The *Enhanced Host Controller Interface (EHCI) For Universal Serial Bus Specification*, Section 4.3 describes the details of Port Suspend and Resume.

3.17.7.3 ACPI Device States

The USB 2.0 function only supports the D0 and D3 PCI Power Management states.

Notes regarding Intel® Xeon® Processor D-1500 Product Family implementation of the Device States:

1. The EHC hardware does not inherently consume any more power when it is in the D0 state than it does in the D3 state. However, software is required to suspend or disable all ports prior to entering the D3 state such that the maximum power consumption is reduced.
2. In the D0 state, all implemented EHC features are enabled.
3. In the D3 state, accesses to the EHC memory-mapped I/O range will master abort. Since the Debug Port uses the same memory range, the Debug Port is only operational when the EHC is in the D0 state.
4. In the D3 state, the EHC interrupt must never assert for any reason. The internal PME# signal is used to signal wake events, and so on.
5. When the Device Power State field is written to D0 from D3, an internal reset is generated. See Section 3.17.1.3, "EHC Resets" for general rules on the effects of this reset.
6. Attempts to write any other value into the Device Power State field other than 00b (D0 state) and 11b (D3 state) will complete normally without changing the current value in this field.

3.17.7.4 ACPI System States

The EHC behavior as it relates to other power management states in the system is summarized in the following list:

- The System is always in the S0 state when the EHC is in the D0 state. However, when the EHC is in the D3 state, the system may be in any power management state (including S0).
- When in D0, the Pause feature (See Section 3.17.7.1) enables dynamic processor low-power states to be entered.
- The PLL in the EHC is disabled when entering the S4/S5 states (core power turns off).
- All core well logic is reset in the S4/S5 states.

3.17.8 USB 2.0 Legacy Keyboard Operation

Intel® Xeon® Processor D-1500 Product Family must support the possibility of a keyboard downstream from either a full-speed/low-speed or a high-speed port. The description of the legacy keyboard support is unchanged from USB 1.1.

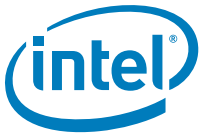
The EHC provides the basic ability to generate SMIs on an interrupt event, along with more sophisticated control of the generation of SMIs.

3.17.9 USB 2.0 Based Debug Port

Intel® Xeon® Processor D-1500 Product Family supports the elimination of the legacy COM ports by providing the ability for debugger software to interact with devices on a USB 2.0 port.

High-level restrictions and features are:

- Operational before USB 2.0 drivers are loaded.
- Functions even when the port is disabled.



- Allows normal system USB 2.0 traffic in a system that may only have one USB port.
- Debug Port device (DPD) must be high-speed capable and connect directly to Port 1 on Intel® Xeon® Processor D-1500 Product Family-based systems (such as, the DPD cannot be connected to
  Port 1 through a hub. When a DPD is detected Intel® Xeon® Processor D-1500 Product Family EHCI will bypass the integrated Rate Matching Hub and connect directly to the port and the DPD.).
- Debug Port FIFO always makes forward progress (a bad status on USB is simply presented back to software).
- The Debug Port FIFO is only given one USB access per microframe.

The Debug port facilitates operating system and device driver debug. It allows the software to communicate with an external console using a USB 2.0 connection. Because the interface to this link does not go through the normal USB 2.0 stack, it allows communication with the external console during cases where the operating system is not loaded, the USB 2.0 software is broken, or where the USB 2.0 software is being debugged. Specific features of this implementation of a debug port are:

- Only works with an external USB 2.0 debug device (console)
- Implemented for a specific port on the host controller
- Operational anytime the port is not suspended AND the host controller is in D0 power state.
- Capability is interrupted when port is driving USB RESET

3.17.9.1 Theory of Operation

There are two operational modes for the USB debug port:

1. Mode 1 is when the USB port is in a disabled state from the viewpoint of a standard host controller driver. In Mode 1, the Debug Port controller is required to generate a "keepalive" packets less than 2 ms apart to keep the attached debug device from suspending. The keepalive packet should be a standalone 32-bit SYNC field.
2. Mode 2 is when the host controller is running (that is, host controller's *Run/Stop#* bit is 1). In Mode 2, the normal transmission of SOF packets will keep the debug device from suspending.

Behavioral Rules

1. In both modes 1 and 2, the Debug Port controller must check for software requested debug transactions at least every 125 microseconds.
2. If the debug port is enabled by the debug driver, and the standard host controller driver resets the USB port, USB debug transactions are held off for the duration of the reset and until after the first SOF is sent.
3. If the standard host controller driver suspends the USB port, then USB debug transactions are held off for the duration of the suspend/resume sequence and until after the first SOF is sent.
4. The ENABLED_CNT bit in the debug register space is independent of the similar port control bit in the associated Port Status and Control register.

Table 3-39 shows the debug port behavior related to the state of bits in the debug registers as well as bits in the associated Port Status and Control register.

Table 3-39. Debug Port Behavior

OWNER_CNT	ENABLED_CT	Port Enable	Run / Stop	Suspend	Debug Port Behavior
0	X	X	X	X	Debug port is not being used. Normal operation.
1	0	X	X	X	Debug port is not being used. Normal operation.
1	1	0	0	X	Debug port in Mode 1. SYNC keepalives sent plus debug traffic
1	1	0	1	X	Debug port in Mode 2. SOF (and only SOF) is sent as keepalive. Debug traffic is also sent. No other normal traffic is sent out this port, because the port is not enabled.
1	1	1	0	0	Invalid. Host controller driver should never put controller into this state (enabled, not running and not suspended).
1	1	1	0	1	Port is suspended. No debug traffic sent.
1	1	1	1	0	Debug port in Mode 2. Debug traffic is interspersed with normal traffic.
1	1	1	1	1	Port is suspended. No debug traffic sent.

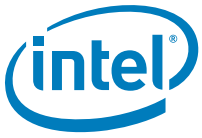
3.17.9.1.1 OUT Transactions

An Out transaction sends data to the debug device. It can occur only when the following are true:

- The debug port is enabled
- The debug software sets the GO_CNT bit
- The WRITE_READ#_CNT bit is set

The sequence of the transaction is:

1. Software sets the appropriate values in the following bits:
   - — USB_ADDRESS_CNF
   - — USB_ENDPOINT_CNF
   - — DATA_BUFFER[63:0]
   - — TOKEN_PID_CNT[7:0]
   - — SEND_PID_CNT[15:8]
   - — DATA_LEN_CNT
   - — WRITE_READ#_CNT: (note: this will always be 1 for OUT transactions)
   - — GO_CNT: (note: this will always be 1 to initiate the transaction)
2. The debug port controller sends a token packet consisting of:
   - — SYNC
   - — TOKEN_PID_CNT field
   - — USB_ADDRESS_CNT field
   - — USB_ENDPOINT_CNT field
   - — 5-bit CRC field
3. After sending the token packet, the debug port controller sends a data packet consisting of:
   - — SYNC



- SEND_PID_CNT field
- The number of data bytes indicated in DATA_LEN_CNT from the DATA_BUFFER
- 16-bit CRC

NOTE: A DATA_LEN_CNT value of 0 is valid in which case no data bytes would be included in the packet.

4. After sending the data packet, the controller waits for a handshake response from the debug device.
   - If a handshake is received, the debug port controller:
     a. Places the received PID in the RECEIVED_PID_STS field
     b. Resets the ERROR_GOOD#_STS bit
     c. Sets the DONE_STS bit
   - If no handshake PID is received, the debug port controller:
     a. Sets the EXCEPTION_STS field to 001b
     b. Sets the ERROR_GOOD#_STS bit
     c. Sets the DONE_STS bit

3.17.9.1.2 IN Transactions

An IN transaction receives data from the debug device. It can occur only when the following are true:

- The debug port is enabled
- The debug software sets the GO_CNT bit
- The WRITE_READ#_CNT bit is reset

The sequence of the transaction is:

1. Software sets the appropriate values in the following bits:
   - USB_ADDRESS_CNF
   - USB_ENDPOINT_CNF
   - TOKEN_PID_CNT[7:0]
   - DATA_LEN_CNT
   - WRITE_READ#_CNT: (note: this will always be 0 for IN transactions)
   - GO_CNT: (note: this will always be 1 to initiate the transaction)
2. The debug port controller sends a token packet consisting of:
   - SYNC
   - TOKEN_PID_CNT field
   - USB_ADDRESS_CNT field
   - USB_ENDPOINT_CNT field
   - 5-bit CRC field.
3. After sending the token packet, the debug port controller waits for a response from the debug device.
   If a response is received:
   - The received PID is placed into the RECEIVED_PID_STS field
   - Any subsequent bytes are placed into the DATA_BUFFER

— The DATA_LEN_CNT field is updated to show the number of bytes that were received after the PID.

4. If a valid packet was received from the device that was one byte in length (indicating it was a handshake packet), then the debug port controller:
   — Resets the ERROR_GOOD#_STS bit
   — Sets the DONE_STS bit
5. If a valid packet was received from the device that was more than one byte in length (indicating it was a data packet), then the debug port controller:
   — Transmits an ACK handshake packet
   — Resets the ERROR_GOOD#_STS bit
   — Sets the DONE_STS bit
6. If no valid packet is received, then the debug port controller:
   — Sets the EXCEPTION_STS field to 001b
   — Sets the ERROR_GOOD#_STS bit
   — Sets the DONE_STS bit.

3.17.9.1.3 Debug Software

Enabling the Debug Port

There are two mutually exclusive conditions that debug software must address as part of its startup processing:

- The EHCI has been initialized by system software
- The EHCI has not been initialized by system software

Debug software can determine the current 'initialized' state of the EHCI by examining the Configure Flag in the EHCI USB 2.0 Command Register. If this flag is set, then system software has initialized the EHCI. Otherwise, the EHCI should not be considered initialized. Debug software will initialize the debug port registers depending on the state of the EHCI. However, before this can be accomplished, debug software must determine which root USB port is designated as the debug port.

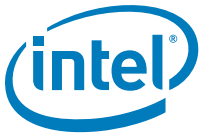
Determining the Debug Port

Debug software can easily determine which USB root port has been designated as the debug port by examining bits 20:23 of the EHCI Host Controller Structural Parameters register. This 4-bit field represents the numeric value assigned to the debug port (that is, 0001=port 1).

Debug Software Startup with Non-Initialized EHCI

Debug software can attempt to use the debug port if after setting the OWNER_CNT bit, the Current Connect Status bit in the appropriate (See *Determining the Debug Port Presence*) PORTSC register is set. If the Current Connect Status bit is not set, then debug software may choose to terminate or it may choose to wait until a device is connected.

If a device is connected to the port, then debug software must reset/enable the port. Debug software does this by setting and then clearing the Port Reset bit the PORTSC register. To ensure a successful reset, debug software should wait at least 50 ms before



clearing the Port Reset bit. Due to possible delays, this bit may not change to 0 immediately; reset is complete when this bit reads as 0. Software must not continue until this bit reads 0.

If a high-speed device is attached, the EHCI will automatically set the Port Enabled/Disabled bit in the PORTSC register and the debug software can proceed. Debug software should set the ENABLED_CNT bit in the Debug Port Control/Status register, and then reset (clear) the Port Enabled/Disabled bit in the PORTSC register (so that the system host controller driver does not see an enabled port when it is first loaded).

Debug Software Startup with Initialized EHCI

Debug software can attempt to use the debug port if the Current Connect Status bit in the appropriate (See Determining the Debug Port) PORTSC register is set. If the Current Connect Status bit is not set, then debug software may choose to terminate or it may choose to wait until a device is connected.

If a device is connected, then debug software must set the OWNER_CNT bit and then the ENABLED_CNT bit in the Debug Port Control/Status register.

Determining Debug Peripheral Presence

After enabling the debug port functionality, debug software can determine if a debug peripheral is attached by attempting to send data to the debug peripheral. If all attempts result in an error (Exception bits in the Debug Port Control/Status register indicates a Transaction Error), then the attached device is not a debug peripheral. If the debug port peripheral is not present, then debug software may choose to terminate or it may choose to wait until a debug peripheral is connected.

3.17.10 EHCI Caching

EHCI Caching is a power management feature in the USB (EHCI) host controllers which enables the controller to execute the schedules entirely in cache and eliminates the need for the DMA engine to access memory when the schedule is idle. EHCI caching allows the processor to maintain longer C-state residency times and provides substantial system power savings.

3.17.11 Intel® USB Pre-Fetch Based Pause

The Intel USB Pre-Fetch Based Pause is a power management feature in USB (EHCI) host controllers to ensure maximum C3/C4 processor power state time with C2 popup. This feature applies to the period schedule, and works by allowing the DMA engine to identify periods of idleness and preventing the DMA engine from accessing memory when the periodic schedule is idle. Typically in the presence of periodic devices with multiple millisecond poll periods, the periodic schedule will be idle for several frames between polls.

The Intel USB Pre-Fetch Based Pause feature is disabled by setting bit 4 of EHCI Configuration Register Section 10.2.1.

3.17.12 Function Level Reset Support (FLR)

The USB EHCI Controllers support the Function Level Reset (FLR) capability. The FLR capability can be used in conjunction with Intel Virtualization Technology. FLR allows an Operating System in a Virtual Machine to have complete control over a device, including its initialization, without interfering with the rest of the platform. The device provides a software interface that enables the Operating System to reset the whole device as if a platform reset was asserted.

3.17.12.1 FLR Steps

3.17.12.1.1 FLR Initialization

1. A FLR is initiated by software writing a '1' to the Initiate FLR bit.
2. All subsequent requests targeting the Function will not be claimed and will be Master Abort Immediate on the bus. This includes any configuration, I/O or Memory cycles, however, the Function shall continue to accept completions targeting the Function.

3.17.12.1.2 FLR Operation

The Function will Reset all configuration, I/O and memory registers of the Function except those indicated otherwise and reset all internal states of the Function to the default or initial condition.

3.17.12.1.3 FLR Completion

The Initiate FLR bit is reset (cleared) when the FLR reset is completed. This bit can be used to indicate to the software that the FLR reset is completed.

Note: From the time Initiate FLR bit is written to 1, software must wait at least 100 ms before accessing the function.

3.17.13 USB Overcurrent Protection

Intel® Xeon® Processor D-1500 Product Family has implemented programmable USB Overcurrent signals. Intel® Xeon® Processor D-1500 Product Family provides a total of 8 overcurrent pins to be shared across the 4 USB 2.0 and 4 USB 3.0 ports.

Each pin is mapped to one or more ports by setting bits in the Over-Current Map registers, depending on whether the port is mapped to EHCI or XHCI. Refer to the following sections for more details:

1. EHCI (USB 2.0 Ports): Section 3.17.13, "USB Overcurrent Protection" .
2. XHCI (USB 2.0 Ports): Section 11.2.31, "U2OCM1 - XHCI USB2 Overcurrent Mapping Register1 (USB xHCI—D20:F0)" .
3. XHCI (USB 2.0 Ports): Section 11.2.32, "U2OCM2 - XHCI USB2 Overcurrent Mapping Register 2 (USB xHCI—D20:F0)" .
4. XHCI (USB 3.0 Ports): Section 11.2.33, "U3OCM1 - XHCI USB3 Overcurrent Pin Mapping 1 (USB xHCI—D20:F0)" .
5. XHCI (USB 3.0 Ports): Section 11.2.34, "U3OCM2 - XHCI USB3 Overcurrent Pin Mapping 2 (USB xHCI—D20:F0)" .

It is system BIOS' responsibility to ensure that each port is mapped to only one over current pin. Operation with more than one overcurrent pin mapped to a port is undefined. It is expected that multiple ports are mapped to a single overcurrent pin, however they should be connected at the port and not at Intel® Xeon® Processor D-1500 Product Family pin. Shorting these pins together may lead to reduced test capabilities. By default, two ports are routed to each of the OC[6:0]# pins. OC7# is not used by default.

NOTES:

1. All USB ports routed out of the package must have Overcurrent protection. It is system BIOS responsibility to ensure all used ports have OC protection.
2. USB Ports that are either unused or only routed within the system (such as, that do not connect to a walk-up port) should not have OC pins assigned to them.

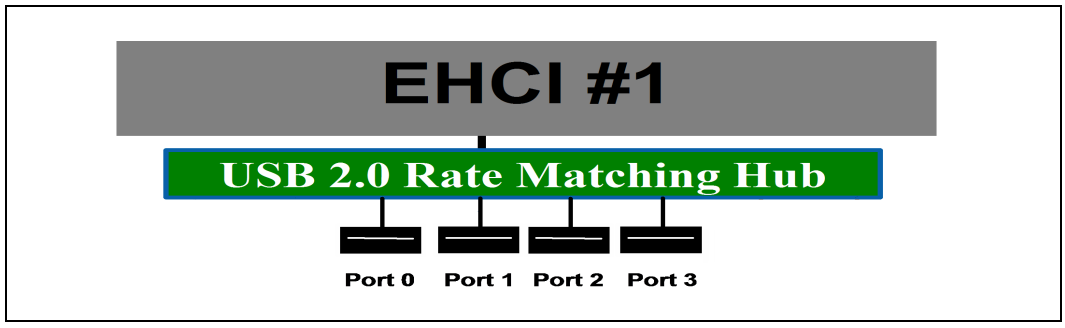
3.18 Integrated USB 2.0 Rate Matching Hub

3.18.1 Overview

Intel® Xeon® Processor D-1500 Product Family has integrated one USB 2.0 Rate Matching Hubs (RMH). One hub is connected to the EHCI controllers as shown in Figure 3-10. The Hub converts low and full-speed traffic into high-speed traffic. When the RMH is enabled, it will appear to software like an external hub is connected to Port 0 of the EHCI controller. In addition, port 1 of each of the RMH is multiplexed with Port 1 of the EHCI controller and is able to bypass the RMH for use as the Debug Port.

The hub operates like any USB 2.0 Discrete Hub and will consume one tier of hubs allowed by the USB 2.0 Specification. Section 4.1.1. A maximum of four additional non-root hubs can be supported on any of Intel® Xeon® Processor D-1500 Product Family USB Ports.

Figure 3-10. EHCI with USB 2.0 with Rate Matching Hub



3.18.2 Architecture

A hub consists of three components: the Hub Repeater, the Hub Controller, and the Transaction Translator.

1. The Hub Repeater is responsible for connectivity setup and tear-down. It also supports exception handling, such as bus fault detection and recovery and connect/disconnect detect.

2. The Hub Controller provides the mechanism for host-to-hub communication. Hub-specific status and control commands permit the host to configure a hub and to monitor and control its individual downstream facing ports.
3. The Transaction Translator (TT) responds to high-speed split transactions and translates them to full-/low-speed transactions with full-/low-speed devices attached on downstream facing ports. There is 1 TT per RMH in Intel® Xeon® Processor D-1500 Product Family.

See Chapter 11 of the USB 2.0 Specification for more details on the architecture of the hubs.

3.19 xHCI Controller (D20:F0)

Intel® Xeon® Processor D-1500 Product Family contains an eXtensible Host Controller Interface (xHCI) host controller which supports up to 4 USB 2.0 ports of which up to 4 can be used as USB 3.0 ports with board routing, ACPI table and BIOS considerations. This controller allows data transfers of up to 5 Gb/s. The controller supports SuperSpeed (SS), high-speed (HS), full-speed (FS) and low speed (LS) traffic on the bus.

The xHCI controller does not have a USB Debug port. If USB debug port functionality is desired then the system SW must use the EHCI-based debug port discussed in Section 3.17.9.

Note: Some USB 3.0 motherboard down devices do not require support for USB 2.0 speed and it is possible to route only the SuperSpeed signals, as allowed by the USB 3.0 specification. In this special case, USB 2.0 and USB 3.0 signals will not need to be paired together, thereby allowing support for more than 4 USB connections.

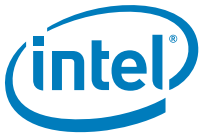
3.20 SMBus Controller (D31:F3)

Intel® Xeon® Processor D-1500 Product Family provides an System Management Bus (SMBus) 2.0 host controller as well as an SMBus Slave Interface. The host controller provides a mechanism for the processor to initiate communications with SMBus peripherals (slaves). Intel® Xeon® Processor D-1500 Product Family is also capable of operating in a mode in which it can communicate with I^2C compatible devices. The host SMBus controller supports up to 100 kHz clock speed.

Intel® Xeon® Processor D-1500 Product Family can perform SMBus messages with either packet error checking (PEC) enabled or disabled. The actual PEC calculation and checking is performed in hardware by Intel® Xeon® Processor D-1500 Product Family.

The Slave Interface allows an external master to read from or write to Intel® Xeon® Processor D-1500 Product Family. Write cycles can be used to cause certain events or pass messages, and the read cycles can be used to determine the state of various status bits. Intel® Xeon® Processor D-1500 Product Family's internal host controller cannot access Intel® Xeon® Processor D-1500 Product Family's internal Slave Interface.

Intel® Xeon® Processor D-1500 Product Family SMBus logic exists in D31:F3 configuration space, and consists of a transmit data path, and host controller. The transmit data path provides the data flow logic needed to implement the seven



different SMBus command protocols and is controlled by the host controller. Intel® Xeon® Processor D-1500 Product Family's SMBus controller logic is clocked by RTC clock.

The SMBus Address Resolution Protocol (ARP) is supported by using the existing host controller commands through software, except for the Host Notify command (which is actually a received message).

The programming model of the host controller is combined into two portions: a PCI configuration portion, and a system I/O mapped portion. All static configuration, such as the I/O base address, is done using the PCI configuration space. Real-time programming of the Host interface is done in system I/O space.

Intel® Xeon® Processor D-1500 Product Family SMBus host controller checks for parity errors as a target. If an error is detected, the detected parity error bit in the PCI Status Register (D31:F3:Offset 06h:Bit 15) is set. If Bit 6 and Bit 8 of the PCI Command Register (D31:F3:Offset 04h) are set, an SERR# is generated and the signaled SERR# bit in the PCI Status Register (bit 14) is set.

3.20.1 Host Controller

The SMBus host controller is used to send commands to other SMBus slave devices. Software sets up the host controller with an address, command, and, for writes, data and optional PEC; and then tells the controller to start. When the controller has finished transmitting data on writes, or receiving data on reads, it generates an SMI# or interrupt, if enabled.

The host controller supports 8 command protocols of the SMBus interface (see *System Management Bus (SMBus) Specification, Version 2.0*): Quick Command, Send Byte, Receive Byte, Write Byte/Word, Read Byte/Word, Process Call, Block Read/Write, Block Write–Block Read Process Call, and Host Notify.

The SMBus host controller requires that the various data and command fields be setup for the type of command to be sent. When software sets the START bit, the SMBus Host controller performs the requested transaction, and interrupts the processor (or generates an SMI#) when the transaction is completed. Once a START command has been issued, the values of the "active registers" (Host Control, Host Command, Transmit Slave Address, Data 0, Data 1) should not be changed or read until the interrupt status message (INTR) has been set (indicating the completion of the command). Any register values needed for computation purposes should be saved prior to issuing of a new command, as the SMBus host controller updates all registers while completing the new command.

Intel® Xeon® Processor D-1500 Product Family supports the *System Management Bus (SMBus) Specification, Version 2.0*. Slave functionality, including the Host Notify protocol, is available on the SMBus pins. The SMLink and SMBus signals can be tied together externally depending on TCO mode used. Refer to Section 3.13.2 for more details.

Using the SMB host controller to send commands to Intel® Xeon® Processor D-1500 Product Family SMB slave port is not supported.

3.20.1.1 Command Protocols

In all of the following commands, the Host Status Register (offset 00h) is used to determine the progress of the command. While the command is in operation, the HOST_BUSY bit is set. If the command completes successfully, the INTR bit will be set in the Host Status Register. If the device does not respond with an acknowledge, and the transaction times out, the DEV_ERR bit is set. If software sets the KILL bit in the Host Control Register while the command is running, the transaction will stop and the FAILED bit will be set.

Quick Command

When programmed for a Quick Command, the Transmit Slave Address Register is sent. The PEC byte is never appended to the Quick Protocol. Software should force the PEC_EN bit to 0 when performing the Quick Command. Software must force the I2C_EN bit to 0 when running this command. See Section 5.5.1 of the *System Management Bus (SMBus) Specification,* Version 2.0 for the format of the protocol.

Send Byte / Receive Byte

For the Send Byte command, the Transmit Slave Address and Device Command Registers are sent. For the Receive Byte command, the Transmit Slave Address Register is sent. The data received is stored in the DATA0 register. Software must force the I2C_EN bit to 0 when running this command.

The Receive Byte is similar to a Send Byte, the only difference is the direction of data transfer. See Sections 5.5.2 and 5.5.3 of the *System Management Bus (SMBus) Specification,* Version 2.0 for the format of the protocol.

Write Byte/Word

The first byte of a Write Byte/Word access is the command code. The next 1 or 2 bytes are the data to be written. When programmed for a Write Byte/Word command, the Transmit Slave Address, Device Command, and Data0 Registers are sent. In addition, the Data1 Register is sent on a Write Word command. Software must force the I2C_EN bit to 0 when running this command. See Section 5.5.4 of the *System Management Bus (SMBus) Specification,* Version 2.0 for the format of the protocol.

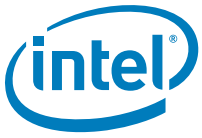
Read Byte/Word

Reading data is slightly more complicated than writing data. First Intel® Xeon® Processor D-1500 Product Family must write a command to the slave device. Then it must follow that command with a repeated start condition to denote a read from that device's address. The slave then returns 1 or 2 bytes of data. Software must force the I2C_EN bit to 0 when running this command.

When programmed for the read byte/word command, the Transmit Slave Address and Device Command Registers are sent. Data is received into the DATA0 on the read byte, and the DAT0 and DATA1 registers on the read word. See Section 5.5.5 of the *System Management Bus (SMBus) Specification,* Version 2.0 for the format of the protocol.

Process Call

The process call is so named because a command sends data and waits for the slave to return a value dependent on that data. The protocol is simply a Write Word followed by a Read Word, but without a second command or stop condition.



When programmed for the Process Call command, Intel® Xeon® Processor D-1500 Product Family transmits the Transmit Slave Address, Host Command, DATA0 and DATA1 registers. Data received from the device is stored in the DATA0 and DATA1 registers. The Process Call command with I2C_EN set and the PEC_EN bit set produces undefined results. Software must force either I2C_EN or PEC_EN to 0 when running this command. See Section 5.5.6 of the *System Management Bus (SMBus) Specification,* Version 2.0 for the format of the protocol.

Note: For process call command, the value written into bit 0 of the Transmit Slave Address Register (SMB I/O register, Offset 04h) needs to be 0.

Note: If the I2C_EN bit is set, the protocol sequence changes slightly: the Command Code (Bits 18:11 in the bit sequence) are not sent - as a result, the slave will not acknowledge (Bit 19 in the sequence).

Block Read/Write

Intel® Xeon® Processor D-1500 Product Family contains a 32-byte buffer for read and write data which can be enabled by setting bit 1 of the Auxiliary Control register at offset 0Dh in I/O space, as opposed to a single byte of buffering. This 32-byte buffer is filled with write data before transmission, and filled with read data on reception. In Intel® Xeon® Processor D-1500 Product Family, the interrupt is generated only after a transmission or reception of 32 bytes, or when the entire byte count has been transmitted/received.

Note: When operating in I^2C* mode (I2C_EN bit is set), Intel® Xeon® Processor D-1500 Product Family will never use the 32-byte buffer for any block commands.

The byte count field is transmitted but ignored by Intel® Xeon® Processor D-1500 Product Family as software will end the transfer after all bytes it cares about have been sent or received.

For a Block Write, software must either force the I2C_EN bit or both the PEC_EN and AAC bits to 0 when running this command.

The block write begins with a slave address and a write condition. After the command code Intel® Xeon® Processor D-1500 Product Family issues a byte count describing how many more bytes will follow in the message. If a slave had 20 bytes to send, the first byte would be the number 20 (14h), followed by 20 bytes of data. The byte count may not be 0. A Block Read or Write is allowed to transfer a maximum of 32 data bytes.

When programmed for a block write command, the Transmit Slave Address, Device Command, and Data0 (count) registers are sent. Data is then sent from the Block Data Byte register; the total data sent being the value stored in the Data0 Register. On block read commands, the first byte received is stored in the Data0 register, and the remaining bytes are stored in the Block Data Byte register. See Section 5.5.7 of the *System Management Bus (SMBus) Specification,* Version 2.0 for the format of the protocol.

Note: For Block Write, if the I2C_EN bit is set, the format of the command changes slightly. Intel® Xeon® Processor D-1500 Product Family will still send the number of bytes (on writes) or receive the number of bytes (on reads) indicated in the DATA0 register. However, it will not send the contents of the DATA0 register as part of the message. Also, the Block Write protocol sequence changes slightly: the Byte Count (bits 27:20 in the bit sequence) are not sent - as a result, the slave will not acknowledge (bit 28 in the sequence).

I²C Read

This command allows Intel® Xeon® Processor D-1500 Product Family to perform block reads to certain I²C* devices, such as serial E²PROMs. The SMBus Block Read supports the 7-bit addressing mode only.

However, this does not allow access to devices using the I²C "Combined Format" that has data bytes after the address. Typically these data bytes correspond to an offset (address) within the serial memory chips.

Note: This command is supported independent of the setting of the I2C_EN bit. The I²C Read command with the PEC_EN bit set produces undefined results. Software must force both the PEC_EN and AAC bit to 0 when running this command.

For I²C Read command, the value written into bit 0 of the Transmit Slave Address Register (SMB I/O register, offset 04h) needs to be 0.

The format that is used for the command is shown in Table 3-40.

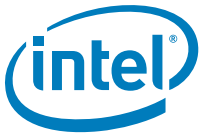
Table 3-40. I²C* Block Read

Bit	Description
1	Start
8:2	Slave Address – 7 bits
9	Write
10	Acknowledge from slave
18:11	Send DATA1 register
19	Acknowledge from slave
20	Repeated Start
27:21	Slave Address – 7 bits
28	Read
29	Acknowledge from slave
37:30	Data byte 1 from slave – 8 bits
38	Acknowledge
46:39	Data byte 2 from slave – 8 bits
47	Acknowledge
–	Data bytes from slave / Acknowledge
–	Data byte N from slave – 8 bits
–	NOT Acknowledge
–	Stop

Intel® Xeon® Processor D-1500 Product Family will continue reading data from the peripheral until the NAK is received.

Block Write–Block Read Process Call

The block write-block read process call is a two-part message. The call begins with a slave address and a write condition. After the command code the host issues a write byte count (M) that describes how many more bytes will be written in the first part of the message. If a master has 6 bytes to send, the byte count field will have the value 6 (0000 0110b), followed by the 6 bytes of data. The write byte count (M) cannot be 0.



The second part of the message is a block of read data beginning with a repeated start condition followed by the slave address and a Read bit. The next byte is the read byte count (N), which may differ from the write byte count (M). The read byte count (N) cannot be 0.

The combined data payload must not exceed 32 bytes. The byte length restrictions of this process call are summarized as follows:

- M ≥ 1 byte
- N ≥ 1 byte
- M + N ≤ 32 bytes

The read byte count does not include the PEC byte. The PEC is computed on the total message beginning with the first slave address and using the normal PEC computational rules. It is highly recommended that a PEC byte be used with the Block Write-Block Read Process Call. Software must do a read to the command register (offset 2h) to reset the 32 byte buffer pointer prior to reading the block data register.

There is no STOP condition before the repeated START condition, and that a NACK signifies the end of the read transfer.

Note: E32B bit in the Auxiliary Control register must be set when using this protocol.

See Section 5.5.8 of the *System Management Bus (SMBus) Specification,* Version 2.0 for the format of the protocol.

3.20.2 Bus Arbitration

Several masters may attempt to get on the bus at the same time by driving the SMBDATA line low to signal a start condition. Intel® Xeon® Processor D-1500 Product Family continuously monitors the SMBDATA line. When Intel® Xeon® Processor D-1500 Product Family is attempting to drive the bus to a 1 by letting go of the SMBDATA line, and it samples SMBDATA low, then some other master is driving the bus and Intel® Xeon® Processor D-1500 Product Family will stop transferring data.

If Intel® Xeon® Processor D-1500 Product Family sees that it has lost arbitration, the condition is called a collision. Intel® Xeon® Processor D-1500 Product Family will set the BUS_ERR bit in the Host Status Register, and if enabled, generate an interrupt or SMI#. The processor is responsible for restarting the transaction.

When Intel® Xeon® Processor D-1500 Product Family is a SMBus master, it drives the clock. When Intel® Xeon® Processor D-1500 Product Family is sending address or command as an SMBus master, or data bytes as a master on writes, it drives data relative to the clock it is also driving. It will not start toggling the clock until the start or stop condition meets proper setup and hold time. Intel® Xeon® Processor D-1500 Product Family will also ensure minimum time between SMBus transactions as a master.

Note: Intel® Xeon® Processor D-1500 Product Family supports the same arbitration protocol for both the SMBus and the System Management (SMLink) interfaces.

3.20.3 Bus Timing

3.20.3.1 Clock Stretching

Some devices may not be able to handle their clock toggling at the rate that Intel® Xeon® Processor D-1500 Product Family as an SMBus master would like. They have the capability of stretching the low time of the clock. When Intel® Xeon® Processor D-1500 Product Family attempts to release the clock (allowing the clock to go high), the clock will remain low for an extended period of time.

Intel® Xeon® Processor D-1500 Product Family monitors the SMBus clock line after it releases the bus to determine whether to enable the counter for the high time of the clock. While the bus is still low, the high time counter must not be enabled. Similarly, the low period of the clock can be stretched by an SMBus master if it is not ready to send or receive data.

3.20.3.2 Bus Time Out (Intel® Xeon® Processor D-1500 Product Family as SMBus Master)

If there is an error in the transaction, such that an SMBus device does not signal an acknowledge, or holds the clock lower than the allowed time-out time, the transaction will time out. Intel® Xeon® Processor D-1500 Product Family will discard the cycle and set the DEV_ERR bit. The time out minimum is 25 ms (800 RTC clocks). The time-out counter inside Intel® Xeon® Processor D-1500 Product Family will start after the last bit of data is transferred by Intel® Xeon® Processor D-1500 Product Family and it is waiting for a response.

The 25-ms time-out counter will not count under the following conditions:

1. BYTE_DONE_STATUS bit (SMBus I/O Offset 00h, Bit 7) is set
2. The SECOND_TO_STS bit (TCO I/O Offset 06h, Bit 1) is not set (this indicates that the system has not locked up).

3.20.4 Interrupts / SMI#

Intel® Xeon® Processor D-1500 Product Family SMBus controller uses PIRQB# as its interrupt pin. However, the system can alternatively be set up to generate SMI# instead of an interrupt, by setting the SMBUS_SMI_EN bit (D31:F0:Offset 40h:Bit 1).

Table 3-42 and Table 3-43 specify how the various enable bits in the SMBus function control the generation of the interrupt, Host and Slave SMI, and Wake internal signals. The rows in the tables are additive, which means that if more than one row is true for a particular scenario then the Results for all of the activated rows will occur.

Table 3-41. Enable for SMBALERT#

Event	INTREN (Host Control I/O Register, Offset 02h, Bit 0)	SMB_SMI_EN (Host Configuration Register, D31:F3:Offset 40h, Bit 1)	SMBALERT_DIS (Slave Command I/O Register, Offset 11h, Bit 2)	Result
SMBALERT# asserted low (always reported in Host Status Register, Bit 5)	X	X	X	Wake generated
	X	1	0	Slave SMI# generated (SMBUS_SMI_STS)
	1	0	0	Interrupt generated

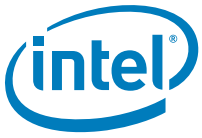


Table 3-42. Enables for SMBus Slave Write and SMBus Host Events

Event	INTREN (Host Control I/O Register, Offset 02h, Bit 0)	SMB_SMI_EN (Host Configuration Register, D31:F3:Offset 40h, Bit 1)	Event
Slave Write to Wake/SMI# Command	X	X	Wake generated when asleep. Slave SMI# generated when awake (SMBUS_SMI_STS).
Slave Write to SMLINK_SLAVE_SMI Command	X	X	Slave SMI# generated when in the S0 state (SMBUS_SMI_STS)
Any combination of Host Status Register [4:1] asserted	0	X	None
	1	0	Interrupt generated
	1	1	Host SMI# generated

Table 3-43. Enables for the Host Notify Command

HOST_NOTIFY_INTREN (Slave Control I/O Register, Offset 11h, Bit 0)	SMB_SMI_EN (Host Config Register, D31:F3:Off40h, Bit 1)	HOST_NOTIFY_WKEN (Slave Control I/O Register, Offset 11h, Bit 1)	Result
0	X	0	None
X	X	1	Wake generated
1	0	X	Interrupt generated
1	1	X	Slave SMI# generated (SMBUS_SMI_STS)

3.20.5 SMBALERT#

SMBALERT# is multiplexed with GPIO[11]. When enable and the signal is asserted, Intel® Xeon® Processor D-1500 Product Family can generate an interrupt, an SMI#, or a wake event from S1–S5.

3.20.6 SMBus CRC Generation and Checking

If the AAC bit is set in the Auxiliary Control register, Intel® Xeon® Processor D-1500 Product Family automatically calculates and drives CRC at the end of the transmitted packet for write cycles, and will check the CRC for read cycles. It will not transmit the contents of the PEC register for CRC. The PEC bit must not be set in the Host Control register if this bit is set, or unspecified behavior will result.

If the read cycle results in a CRC error, the DEV_ERR bit and the CRCE bit in the Auxiliary Status register at Offset 0Ch will be set.

3.20.7 SMBus Slave Interface

Intel® Xeon® Processor D-1500 Product Family SMBus Slave interface is accessed using the SMBus. The SMBus slave logic will not generate or handle receiving the PEC byte and will only act as a Legacy Alerting Protocol device. The slave interface allows

Intel® Xeon® Processor D-1500 Product Family to decode cycles, and allows an external microcontroller to perform specific actions. Key features and capabilities include:

- Supports decode of three types of messages: Byte Write, Byte Read, and Host Notify.
- Receive Slave Address register: This is the address that Intel® Xeon® Processor D-1500 Product Family decodes. A default value is provided so that the slave interface can be used without the processor having to program this register.
- Receive Slave Data register in the SMBus I/O space that includes the data written by the external microcontroller.
- Registers that the external microcontroller can read to get the state of Intel® Xeon® Processor D-1500 Product Family.
- Status bits to indicate that the SMBus slave logic caused an interrupt or SMI# due to the reception of a message that matched the slave address.
  - Bit 0 of the Slave Status Register for the Host Notify command
  - Bit 16 of the SMI Status Register (Section 7.8.3.8) for all others

Note: The external microcontroller should not attempt to access Intel® Xeon® Processor D-1500 Product Family SMBus slave logic until either:

- 800 milliseconds after both: RTCRST# is high and RSMRST# is high, OR
- The PLTRST# de-asserts

If a master leaves the clock and data bits of the SMBus interface at 1 for 50 µs or more in the middle of a cycle, Intel® Xeon® Processor D-1500 Product Family slave logic's behavior is undefined. This is interpreted as an unexpected idle and should be avoided when performing management activities to the slave logic.

Note: When an external microcontroller accesses the SMBus Slave Interface over the SMBus a translation in the address is needed to accommodate the least significant bit used for read/write control. For example, if Intel® Xeon® Processor D-1500 Product Family slave address (RCV_SLVA) is left at 44h (default), the external micro controller would use an address of 88h/89h (write/read).

3.20.7.1 Format of Slave Write Cycle

The external master performs Byte Write commands to Intel® Xeon® Processor D-1500 Product Family SMBus Slave I/F. The "Command" field (bits 11:18) indicate which register is being accessed. The Data field (bits 20:27) indicate the value that should be written to that register.

Table 3-44 has the values associated with the registers.

Table 3-44. Slave Write Registers (Sheet 1 of 2)

Register	Function
0	Command Register. See Table 3-45 for legal values written to this register.
1–3	Reserved
4	Data Message Byte 0
5	Data Message Byte 1
6–7	Reserved
8	Reserved

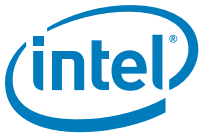


Table 3-44. Slave Write Registers (Sheet 2 of 2)

Register	Function
9–FFh	Reserved

Note: The external microcontroller is responsible to make sure that it does not update the contents of the data byte registers until they have been read by the system processor. Intel® Xeon® Processor D-1500 Product Family overwrites the old value with any new value received. A race condition is possible where the new value is being written to the register just at the time it is being read. Intel® Xeon® Processor D-1500 Product Family will not attempt to cover this race condition (that is, unpredictable results in this case).

Table 3-45. Command Types

Command Type	Description
0	Reserved
1	**WAKE/SMI#.** This command wakes the system if it is not already awake. If system is already awake, an SMI# is generated. ***Note:*** The SMB_WAK_STS bit will be set by this command, even if the system is already awake. The SMI handler should then clear this bit.
2	**Unconditional Powerdown.** This command sets the PWRBTNOR_STS bit, and has the same effect as the Powerbutton Override occurring.
3	**HARD RESET WITHOUT CYCLING:** This command causes a hard reset of the system (does not include cycling of the power supply). This is equivalent to a write to the CF9h register with Bits 2:1 set to 1, but Bit 3 clear to 0.
4	**HARD RESET SYSTEM.** This command causes a hard reset of the system (including cycling of the power supply). This is equivalent to a write to the CF9h register with Bits 3:1 set to 1.
5	**Disable the TCO Messages.** This command will disable Intel® Xeon® Processor D-1500 Product Family from sending Heartbeat and Event messages (as described in Section 3.13). Once this command has been executed, Heartbeat and Event message reporting can only be re-enabled by assertion and de-assertion of the RSMRST# signal.
6	**WD RELOAD:** Reload watchdog timer.
7	Reserved
8	**SMLINK_SLV_SMI.** When Intel® Xeon® Processor D-1500 Product Family detects this command type while in the S0 state, it sets the SMLINK_SLV_SMI_STS bit (see Section 7.9.5). This command should only be used if the system is in an S0 state. If the message is received during S1–S5 states, Intel® Xeon® Processor D-1500 Product Family acknowledges it, but the SMLINK_SLV_SMI_STS bit does not get set. ***Note:*** It is possible that the system transitions out of the S0 state at the same time that the SMLINK_SLV_SMI command is received. In this case, the SMLINK_SLV_SMI_STS bit may get set but not serviced before the system goes to sleep. Once the system returns to S0, the SMI associated with this bit would then be generated. Software must be able to handle this scenario.
9–FFh	Reserved.

3.20.7.2 Format of Read Command

The external master performs Byte Read commands to Intel® Xeon® Processor D-1500 Product Family SMBus Slave interface. The “Command” field (bits 18:11) indicate which register is being accessed. The Data field (bits 30:37) contain the value that should be read from that register.

Table 3-46. Slave Read Cycle Format (Sheet 1 of 2)

Bit	Description	Driven by	Comment
1	Start	External Microcontroller	
2–8	Slave Address - 7 bits	External Microcontroller	Must match value in Receive Slave Address register
9	Write	External Microcontroller	Always 0

Table 3-46. Slave Read Cycle Format (Sheet 2 of 2)

Bit	Description	Driven by	Comment
10	ACK	Intel® Xeon® Processor D-1500 Product Family	
11–18	Command code – 8 bits	External Microcontroller	Indicates which register is being accessed. See Table 3-47 for a list of implemented registers.
19	ACK	Intel® Xeon® Processor D-1500 Product Family	
20	Repeated Start	External Microcontroller	
21–27	Slave Address - 7 bits	External Microcontroller	Must match value in Receive Slave Address register
28	Read	External Microcontroller	Always 1
29	ACK	Intel® Xeon® Processor D-1500 Product Family	
30–37	Data Byte	Intel® Xeon® Processor D-1500 Product Family	Value depends on register being accessed. See Table 3-47 for a list of implemented registers.
38	NOT ACK	External Microcontroller	
39	Stop	External Microcontroller	

Table 3-47. Data Values for Slave Read Registers (Sheet 1 of 2)

Register	Bits	Description
0	7:0	Reserved for capabilities indication. Should always return 00h. Future chips may return another value to indicate different capabilities.
1	2:0	System Power State 000 = S0 001 = S1 010 = Reserved 011 = Reserved 100 = S4 101 = S5 110 = Reserved 111 = Reserved
	7:3	Reserved
2	3:0	Reserved
	7:4	Reserved
3	5:0	**Watchdog Timer current value.** The Watchdog Timer has 10 bits, but this field is only 6 bits. If the current value is greater than 3Fh, Intel® Xeon® Processor D-1500 Product Family will always report 3Fh in this field.
	7:6	Reserved
4	0	1 = The **Intruder Detect** (INTRD_DET) bit is set. This indicates that the system cover has probably been opened.
	1	1 = BTI **Temperature Event** occurred. This bit will be set if Intel® Xeon® Processor D-1500 Product Family THRM# input signal is active. Else this bit will read "0."
	2	**DOA Processor Status**. This bit will be 1 to indicate that the processor is dead
	3	1 = **SECOND_TO_STS** bit set. This bit will be set after the second time-out (SECOND_TO_STS bit) of the Watchdog Timer occurs.
	6:4	Reserved. Will always be 0, but software should ignore.
	7	Reflects the value of the GPIO[11]/SMBALERT# pin (and is dependent upon the value of the GPI_INV[11] bit. If the GPI_INV[11] bit is 1, then the value in this bit equals the level of the GPI[11]/SMBALERT# pin (high = 1, low = 0). If the GPI_INV[11] bit is 0, then the value of this bit will equal the inverse of the level of the GPIO[11]/SMBALERT# pin (high = 0, low = 1).

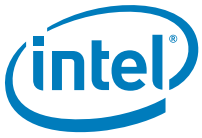


Table 3-47. Data Values for Slave Read Registers (Sheet 2 of 2)

Register	Bits	Description
5	0	**FWH bad bit.** This bit will be 1 to indicate that the FWH read returned FFh, which indicates that it is probably blank.
	1	Reserved
	2	**SYS_PWROK Failure Status:** This bit will be 1 if the SYSPWR_FLR bit in the GEN_PMCON_2 register is set.
	3	Reserved
	4	Reserved
	5	**POWER_OK_BAD:** Indicates the failure core power well ramp during boot/resume. This bit will be active if the SLP_S3# pin is de-asserted and PCH_PWROK pin is not asserted.
	6	**Thermal Trip:** This bit will shadow the state of processor Thermal Trip status bit (CTS) (16.2.1.2, GEN_PMCON_2, bit 3). Events on signal will not create a event message
	7	Reserved: Default value is "X" ***Note:*** Software should not expect a consistent value when this bit is read through SMBUS/SMLink
6	7:0	Contents of the Message 1 register. Refer to Section 7.9.8 for the description of this register.
7	7:0	Contents of the Message 2 register. Refer to Section 7.9.8 for the description of this register.
8	7:0	Contents of the TCO_WDCNT register. Refer to Section 7.9.9 for the description of this register.
9	7:0	Seconds of the RTC
A	7:0	Minutes of the RTC
B	7:0	Hours of the RTC
C	7:0	"Day of Week" of the RTC
D	7:0	"Day of Month" of the RTC
E	7:0	Month of the RTC
F	7:0	Year of the RTC
10h–FFh	7:0	Reserved

3.20.7.2.1 Behavioral Notes

According to SMBus protocol, Read and Write messages always begin with a Start bit – Address– Write bit sequence. When Intel® Xeon® Processor D-1500 Product Family detects that the address matches the value in the Receive Slave Address register, it will assume that the protocol is always followed and ignore the Write bit (Bit 9) and signal an Acknowledge during bit 10. In other words, if a Start –Address–Read occurs (which is illegal for SMBus Read or Write protocol), and the address matches Intel® Xeon® Processor D-1500 Product Family's Slave Address, Intel® Xeon® Processor D-1500 Product Family will still grab the cycle.

Also according to SMBus protocol, a Read cycle contains a Repeated Start–Address–Read sequence beginning at Bit 20. Once again, if the Address matches Intel® Xeon® Processor D-1500 Product Family's Receive Slave Address, it will assume that the protocol is followed, ignore bit 28, and proceed with the Slave Read cycle.

Note: An external microcontroller must not attempt to access Intel® Xeon® Processor D-1500 Product Family's SMBus Slave logic until at least 1 second after both RTCRST# and RSMRST# are de-asserted (high).

3.20.7.3 Slave Read of RTC Time Bytes

Intel® Xeon® Processor D-1500 Product Family SMBus slave interface allows external SMBus master to read the internal RTC's time byte registers.

The RTC time bytes are internally latched by Intel® Xeon® Processor D-1500 Product Family's hardware whenever RTC time is not changing and SMBus is idle. This ensures that the time byte delivered to the slave read is always valid and it does not change when the read is still in progress on the bus. The RTC time will change whenever hardware update is in progress, or there is a software write to the RTC time bytes.

Intel® Xeon® Processor D-1500 Product Family SMBus slave interface only supports Byte Read operation. The external SMBus master will read the RTC time bytes one after another. It is software's responsibility to check and manage the possible time rollover when subsequent time bytes are read.

For example, assuming the RTC time is 11 hours: 59 minutes: 59 seconds. When the external SMBus master reads the hour as 11, then proceeds to read the minute, it is possible that the rollover happens between the reads and the minute is read as 0. This results in 11 hours: 0 minute instead of the correct time of 12 hours: 0 minutes. Unless it is certain that rollover will not occur, software is required to detect the possible time rollover by reading multiple times such that the read time bytes can be adjusted accordingly
if needed.

3.20.7.4 Format of Host Notify Command

Intel® Xeon® Processor D-1500 Product Family tracks and responds to the standard Host Notify command as specified in the *System Management Bus (SMBus) Specification,* Version 2.0. The host address for this command is fixed to 0001000b. If Intel® Xeon® Processor D-1500 Product Family already has data for a previously-received host notify command which has not been serviced yet by the host software (as indicated by the HOST_NOTIFY_STS bit), then it will NACK following the host address byte of the protocol. This allows the host to communicate non-acceptance to the master and retain the host notify address and data values for the previous cycle until host software completely services the interrupt.

Note: Host software must always clear the HOST_NOTIFY_STS bit after completing any necessary reads of the address and data registers.

Table 3-48 shows the Host Notify format.

Table 3-48. Host Notify Format (Sheet 1 of 2)

Bit	Description	Driven By	Comment
1	Start	External Master	
8:2	SMB Host Address – 7 bits	External Master	Always 0001_000
9	Write	External Master	Always 0
10	ACK (or NACK)	Intel® Xeon® Processor D-1500 Product Family	Intel® Xeon® Processor D-1500 Product Family NACKs if HOST_NOTIFY_STS is 1
17:11	Device Address – 7 bits	External Master	Indicates the address of the master; loaded into the Notify Device Address Register
18	Unused – Always 0	External Master	7-bit-only address; this bit is inserted to complete the byte

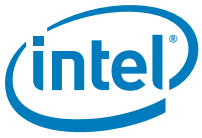


Table 3-48. Host Notify Format (Sheet 2 of 2)

Bit	Description	Driven By	Comment
19	ACK	Intel® Xeon® Processor D-1500 Product Family	
27:20	Data Byte Low – 8 bits	External Master	Loaded into the Notify Data Low Byte Register
28	ACK	Intel® Xeon® Processor D-1500 Product Family	
36:29	Data Byte High – 8 bits	External Master	Loaded into the Notify Data High Byte Register
37	ACK	Intel® Xeon® Processor D-1500 Product Family	
38	Stop	External Master	

3.21 Thermal Management

3.21.1 Thermal Sensor

Intel® Xeon® Processor D-1500 Product Family incorporates one on-die Digital thermal sensor (DTS) for thermal management. The thermal sensor can provide Intel® Xeon® Processor D-1500 Product Family temperature information to an EC or SIO device that can be used to determine how to control the fans.

The on-die thermal sensor is placed as close as possible to the hottest on-die location to reduce thermal gradients and to reduce the error on the sensor trip thresholds. The thermal sensor trip points may be programmed to generate various interrupts including SCI, SMI and other General Purpose events.

3.21.1.1 Internal Thermal Sensor Operation

The internal thermal sensor reports four trip points: Aux2, Aux, Hot and Catastrophic trip points in the order of increasing temperature.

Aux, Aux2 Temperature Trip Points

These trip points may be set dynamically if desired and provides an interrupt to ACPI (or other software) when it is crossed in either direction. These auxiliary temperature trip points do not automatically cause any hardware throttling but may be used by software to trigger interrupts. This trip point is set below the Hot temperature trip point and responses are separately programmable from the hot temperature settings, in order to provide incrementally more aggressive actions. Aux and Aux2 trip points are fully Software programmable during system run-time. Aux2 trip point is set below the Aux temperature trip point.

Hot Temperature Trip Point

This trip point may be set dynamically if desired and provides an interrupt to ACPI (or other software) when it is crossed in either direction. Software could optionally set this as an Interrupt when the temperature exceeds this level setting. Hot trip does not provide any default hardware based thermal throttling, and is available only as a customer configurable interrupt when Tj,max has been reached.

Catastrophic Trip Point

This trip point is set at the temperature at which Intel® Xeon® Processor D-1500 Product Family must be shut down immediately without any software support. The catastrophic trip point must correspond to a temperature ensured to be functional in order for the interrupt generation and Hardware response. Hardware response using THRMTRIP# would be an unconditional transition to S5. The catastrophic transition to the S5 state does not enforce a minimum time in the S5 state. It is assumed that the S5 residence and the reboot sequence cools down the system. If the catastrophic condition remains when the catastrophic power down enable bit is set by BIOS, then the system will re-enter S5.

Thermometer Mode

The thermometer is implemented using a counter that starts at 0 and increments during each sample point until the comparator indicates the temperature is above the current value. The value of the counter is loaded into a read-only register (Thermal Sensor Thermometer Read) when the comparator first trips.

3.21.1.1.1 Recommended Programming for Available Trip Points

There may be a ±2 °C offset due to thermal gradient between the hot-spot and the location of the thermal sensor. Trip points should be programmed to account for this temperature offset between the hot-spot Tj,max and the thermal sensor.

Aux Trip Points should be programmed for software and firmware control using interrupts.

Hot Trip Point should be set to throttle at 108 °C (Tj,max) due to DTS trim accuracy adjustments. Hot trip points should also be programmed for a software response.

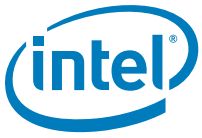
Catastrophic Trip Point should be set to halt operation to avoid maximum Tj of about 120 °C.

Note: Crossing a trip point in either direction may generate several types of interrupts. Each trip point has a register that can be programmed to select the type of interrupt to be generated. Crossing a trip point is implemented as edge detection on each trip point to generate the interrupts.

3.21.1.1.2 Thermal Sensor Accuracy ($T_{accuracy}$)

Taccuracy for Intel® Xeon® Processor D-1500 Product Family is ±5 °C in the temperature range 90 °C to 120 °C. Taccuracy is ±10 °C for temperatures from 45 °C – 90 °C. Intel® Xeon® Processor D-1500 Product Family may not operate above +108 °C. This value is based on product characterization and is not ensured by manufacturing test.

Software has the ability to program the Tcat, Thot, and Taux trip points, but these trip points should be selected with consideration for the thermal sensor accuracy and the quality of the platform thermal solution. Overly conservative (unnecessarily low) temperature settings may unnecessarily degrade performance due to frequent throttling, while overly aggressive (dangerously high) temperature settings may fail to protect the part against permanent thermal damage.



3.21.2 Intel® Xeon® Processor D-1500 Product Family Thermal Throttling

Occasionally Intel® Xeon® Processor D-1500 Product Family may operate in conditions that exceed its maximum operating temperature. In order to protect itself and the system from thermal failure, Intel® Xeon® Processor D-1500 Product Family is capable of reducing its overall power consumption and as a result, lower its temperature. This is achieved by:

- Forcing the SATA device and interface in to a lower power state
- Reducing the Intel Management Engine (Intel ME) clock frequency

The severity of the throttling response is defined by four global Intel® Xeon® Processor D-1500 Product Family throttling states referred to as T-states. In each T-state, the throttling response will differ per interface, but will operate concurrently when a global T-state is activated. A T-state corresponds to a temperature range. The T-states are defined in Table 3-49.

Table 3-49. Intel® Xeon® Processor D-1500 Product Family Thermal Throttle States (T-states)

State	Description
T0	Normal operation, temperature is less than the T1 trip point temperature
T1	Temperature is greater than or equal to the T1 trip point temperature, but less than the T2 trip point temperature. The default temperature is $T_{j,max}$ at 108 °C
T2	Temperature is greater than or equal to the T2 trip point temperature, but less than the T3 trip point temperature. The default temperature is 112 °C
T3	Temperature is greater than or equal to the T3 trip point temperature. The default temperature is 116 °C

Enabling of this feature requires appropriate Intel® Management Engine firmware and configuration of the following registers shown in Table 3-50.

Table 3-50. Intel® Xeon® Processor D-1500 Product Family Thermal Throttling Configuration Registers

Register Name	Register Location	
TL – Throttle Levels	TBARB+40h	Section 16.2.10

3.21.3 Thermal Reporting Over System Management Link 1 Interface (SMLink0)

SMLink0 interface in Intel® Xeon® Processor D-1500 Product Family is the SMBus link to an optional external controller. A SMBus protocol is defined on Intel® Xeon® Processor D-1500 Product Family to allow compatible devices such as Embedded Controller (EC) or SIO to obtain system thermal data from Intel® Xeon® Processor D-1500 Product Family sensors using the SMLink0 interface. This solution allows an external device or controller to use the system thermal data for system thermal management.

Note: To enable Thermal Reporting: Set Section 16.2.4, "TSEL — Thermal Sensor Enable and Lock Register" bit 0 = 1 (Enable TS) and Section 16.2.5, "TSREL—Thermal Sensor Reporting Enable and Lock Register" bit 0 = 1 (Enable SMBus Temperature Reporting).

There are two uses for Intel® Xeon® Processor D-1500 Product Family's thermal reporting capability:

1. To provide system thermal data to an external controller. The controller can manage the fans and other cooling elements based on this data. In addition, Intel® Xeon® Processor D-1500 Product Family can be programmed by setting appropriate bits in the Section 16.2.7, "CTT—Catastrophic Trip Point Register" , Section 16.2.8, "TAHV—Thermal Alert High Value Register" and Section 16.2.9, "TALV—Thermal Alert Low Value Register" to alert the controller when a device has gone outside of its temperature limits. The alert causes the assertion of Intel® Xeon® Processor D-1500 Product Family TEMP_ALERT# (SML1ALERT#/ TEMP_ALERT#/GPIO74) signal. See Section 3.21.3.5 for more details.
2. To provide an interface between the external controller and host software. This software interface has no direct affect on Intel® Xeon® Processor D-1500 Product Family's thermal collection. It is strictly a software interface to pass information or data.

Intel® Xeon® Processor D-1500 Product Family responds to thermal requests only when the system is in S0 or S1. Once Intel® Xeon® Processor D-1500 Product Family has been programmed, it will start responding to a request while the system is in S0 or S1.

To implement this thermal reporting capability, the platform is required to have appropriate BIOS support and compatible devices that support the SMBus protocol.

3.21.3.1 Block Read Address

Intel® Xeon® Processor D-1500 Product Family supports the Block Read Address for reads. This address is used for reads from Intel® Xeon® Processor D-1500 Product Family.

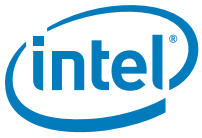
- The address is set by soft straps or BIOS. It can be set to any value the platform requires.
- This address only supports SMBus Block Read command and not Byte or Word Read.
- The Block Read command is supported as defined in the SMBus 2.0 specification, with the command being 44h, and the byte count being provided by Intel® Xeon® Processor D-1500 Product Family following the block read format in the SMBus specification.
- Writes are not allowed to this address, and result in indeterminate behavior.
- Packet Error Code (PEC) may be enabled or not, which is set up by BIOS.

3.21.3.2 Block Read Command

The external controller may read thermal information from Intel® Xeon® Processor D-1500 Product Family using the SMBus Block Read Command. Byte-read and Word-read SMBus commands are not supported. The reads use a different address than the writes.

The command format follows the Block Read format of the SMBus specification.

Intel® Xeon® Processor D-1500 Product Family returns a single byte of data, indicating the temperature between 0 °C (0x00) and 254 °C (0xFE). A read of 0xFF indicates that the sensor is not yet enabled. For more information, see Section 3.21.3.3.1.



3.21.3.3 Read Data Format

For each of the data fields an ERROR Code is listed below. This code indicates that Intel® Xeon® Processor D-1500 Product Family failed in its access to the device. This would be for the case where the read returned no data, or some illegal value. In general that would mean the device is broken. The EC can treat the device that failed the read as broken or with some fail-safe mechanism.

3.21.3.3.1 Intel® Xeon® Processor D-1500 Product Family Temperature

The temperature readings for Intel® Xeon® Processor D-1500 Product Family are 8-bit unsigned values from 0–255. The minimum granularity supported by the internal thermal sensor is 1 °C. Thus, there are no fractional values for Intel® Xeon® Processor D-1500 Product Family temperatures. The device returns a temperature between 0 °C (0x00) and 254 °C (0xFE). Devices that are not yet enabled return the value 0xFF.

Note: Sensors used within the components do not support values below 0°C, so this field is treated as 8 bits (0-255) absolute.

3.21.3.4 Thermal Data Update Rate

The temperature values are updated every 1 ms in Intel® Xeon® Processor D-1500 Product Family, so reading more often than that simply returns the same data multiple times. Also, the data may be up to 1 ms old if the external controller reads the data right before the next update window.

3.21.3.5 Temperature Comparator and Alert

Intel® Xeon® Processor D-1500 Product Family has the ability to alert the external controller when temperatures are out of range. This is done using Intel® Xeon® Processor D-1500 Product Family TEMP_ALERT# signal. The alert is a simple comparator. If any device's temperature is outside the limit range for that device, then the signal is asserted (electrical low). This alert does not use the SML1ALERT#.

Intel® Xeon® Processor D-1500 Product Family supports 2 ranges: an upper and lower limit (8 bits each, in degrees C) for Intel® Xeon® Processor D-1500 Product Family temperature.

The comparator checks if the device is within the specified range, including the limits. For example, a device that is at 100 degrees when the upper limit is 100 will not trigger the alert. Likewise, a device that is at 70 degrees when the lower limit is 70 will not trigger the alert.

The compares are done only on devices that have been enabled by BIOS for checking.

The compares are done in firmware, so all the compares are executed in one software loop and at the end, if there is any out of bound temperature, Intel® Xeon® Processor D-1500 Product Family’s TEMP_ALERT# signal is asserted.

When the external controller sees the TEMP_ALERT# signal low, it knows the device is out of range. It can read the temperature and then change the limit for the device. It may take up to 250 ms before the actual writes cause the signal to change state. For instance, if Intel® Xeon® Processor D-1500 Product Family is at 105 degrees and the limit is 100, the alert is triggered. If the controller changes the limits to 110, the

TEMP_ALERT# signal may remain low until the next thermal sampling window (every 1 ms) occurs and only then go high, assuming Intel® Xeon® Processor D-1500 Product Family was still within its limits.

At boot, the controller can monitor the TEMP_ALERT# signal state. When BIOS has finished all the initialization and enabled the temperature comparators, the TEMP_ALERT# signal will be asserted since the default state of the limit registers is 0h; hence, when Intel® Xeon® Processor D-1500 Product Family first reads temperatures, they will be out of range. This is the positive indication that the external controller may now read thermal information and get valid data. If the TEMP_ALERT# signal is enabled and not asserted within 30 seconds after PLTRST#, the external controller should assume there is a fatal error and handle accordingly. In general the TEMP_ALERT# signal will assert within a 1–4 seconds, depending on the actual BIOS implementation and flow.

Note: The TEMP_ALERT# assertion is only valid when PLTRST# is de-asserted. The controller should mask the state of this signal when PLTRST# is asserted. Since the controller may be powered even when Intel® Xeon® Processor D-1500 Product Family and the rest of the platform are not, the signal may glitch as power is being asserted; thus, the controller should wait until PLTRST# has de-asserted before monitoring the signal.

3.21.3.5.1 Special Conditions

The external controller should have a graceful means of handling when TEMP_ALERT# asserts, and the controller reads Intel® Xeon® Processor D-1500 Product Family, but all temperature values are within limits. In this case, the controller should assume that by the time the controller could read the data, it had changed and moved back within the limits.

3.21.3.6 BIOS Set Up

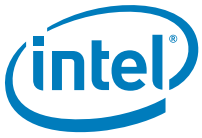
In order for Intel® Xeon® Processor D-1500 Product Family to properly report temperature and enable alerts, the BIOS must configure Intel® Xeon® Processor D-1500 Product Family at boot or from suspend/resume state by writing the following information to Intel® Xeon® Processor D-1500 Product Family MMIO space. This information is NOT configurable using the external controller.

- Enables for Intel® Xeon® Processor D-1500 Product Family thermal alerts.
- Enables for reading Intel® Xeon® Processor D-1500 Product Family temperatures.
- Setting up the temperature calculation equations.

3.21.3.7 SMBus Rules

Intel® Xeon® Processor D-1500 Product Family may NACK an incoming SMBus transaction. In certain cases Intel® Xeon® Processor D-1500 Product Family will NACK the address, and in other cases it will NACK the command depending on internal conditions (such as errors, busy conditions). Given that most of the cases are due to internal conditions, the external controller must alias a NACK of the command and a NACK of the address to the same behavior. The controller must not try to make any determination of the reason for the NACK, based on the type of NACK (command versus address).

Intel® Xeon® Processor D-1500 Product Family will NACK when it is enabled but busy. The external controller is required to retry up to 3 times when they are NACK'ed. In reality if there is a NACK because of Intel® Xeon® Processor D-1500 Product Family



being busy, in almost all cases the next read will succeed since the update internally takes very little time. In the case of a long delay, the external controller must assume that Intel® Xeon® Processor D-1500 Product Family will never return good data.

3.21.3.7.1 During Block Read

On the Block Read, Intel® Xeon® Processor D-1500 Product Family will respect the NACK and Stop indications from the external controller, but will consider this an error case. It will recover from this case and correctly handle the next SMBus request.

Intel® Xeon® Processor D-1500 Product Family will honor STOP during the block read command and cease providing data. On the next Block Read, the data will start with byte 0 again. However, this is not a recommended usage except for 'emergency cases'. In general the external controller should read the entire length of data that was originally programmed.

3.21.3.7.2 Power On

On the Block Read, Intel® Xeon® Processor D-1500 Product Family will respect the NACK and Stop indications from the external controller, but will consider this an error case. It will recover from this case and correctly handle the next SMBus request.

Intel® Xeon® Processor D-1500 Product Family will honor STOP during the block read command and cease providing data. On the next Block Read, the data will start with byte 0 again. However, this is not a recommended usage except for 'emergency cases'. In general the external controller should read the entire length of data that was originally programmed.

3.21.3.8 Case for Considerations

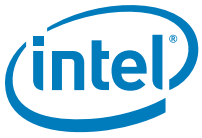
Below are some corner cases and some possible actions that the external controller could take.

A 1-byte sequence number is available to the data read by the external controller. Each time Intel® Xeon® Processor D-1500 Product Family updates the thermal information it will increment the sequence number. The external controller can use this value as an indication that the thermal FW is actually operating. The sequence number will roll over to 00h when it reaches FFh.

1. Power on:
   a. Intel® Xeon® Processor D-1500 Product Family will not respond to any SMBus activity (on SMLink0 interface) until it has loaded the thermal Firmware (FW), which in general would take 1–4 ms. During this period, Intel® Xeon® Processor D-1500 Product Family will NACK any SMBus transaction from the external controller.
   b. The load should take 1-4 ms, but the external controller should design for 30 seconds based on long delays for S4 resume which takes longer than normal power up. This would be an extreme case, but for larger memory footprints and non-optimized recovery times, 30 seconds is a safe number to use for the time-out.
   c. Recover/Failsafe: if Intel® Xeon® Processor D-1500 Product Family has not responded within 30 seconds, the external controller can assume that the system has had a major error and the external controller should ramp the fans to some reasonably high value.
   The only recover from this is an internal reset on Intel® Xeon® Processor D-1500 Product Family, which is not visible to the external controller. Therefore the

external controller might choose to poll every 10-60 seconds (some fairly long period) hereafter to see if Intel® Xeon® Processor D-1500 Product Family's thermal reporting has come alive.

2. Intel® Xeon® Processor D-1500 Product Family Thermal FW hangs and requires an internal reset which is not visible to the external controller.
   a. Intel® Xeon® Processor D-1500 Product Family will NACK any SMBus transaction from the external controller. Intel® Xeon® Processor D-1500 Product Family may not be able to respond for up to 30 seconds while the FW is being reset and reconfigured.
      The external controller could choose to poll every 1-10 seconds to see if the thermal FW has been successfully reset and is now providing data.
   b. General recovery for this case is about 1 second, but 30 seconds should be used by the external controller at the time-out.
   c. Recovery/Failsafe: same as in case #1.
3. Fatal Intel® Xeon® Processor D-1500 Product Family error, causes a global reset of all components.
   a. When there is a fatal Intel® Xeon® Processor D-1500 Product Family error, a global reset may occur, and then case #1 applies.
      The external controller can observe, if desired, PLTRST# assertion as an indication of this event.
4. Intel® Xeon® Processor D-1500 Product Family thermal FW fails or is hung, but no reset occurs
   a. The sequence number will not be updated, so the external controller knows to go to failsafe after some number of reads (8 or so) return the same sequence number.
      The external controller could choose to poll every 1-10 seconds to see if the thermal FW has been successfully reset and working again.
   b. In the absence of other errors, the updates for the sequence number should never be longer than 400 ms, so the number of reads needed to indicate that there is a hang should be at around 2 seconds. But when there is an error, the sequence number may not get updated for seconds. In the case that the external controller sees a NACK from Intel® Xeon® Processor D-1500 Product Family, then it should restart its sequence counter, or otherwise be aware that the NACK condition needs to be factored into the sequence number usage.
   c. The use of sequence numbers is not required, but is provided as a means to ensure correct Intel® Xeon® Processor D-1500 Product Family FW operation.
5. When Intel® Xeon® Processor D-1500 Product Family updates the Block Read data structure, the external controller gets a NACK during this period.
   a. To ensure atomicity of the SMBus data read with respect to the data itself, when the data buffer is being updated, Intel® Xeon® Processor D-1500 Product Family will NACK the Block Read transaction.
   b. The update is only a few micro-seconds, so very short in terms of SMBus polling time; therefore, the next read should be successful. The external controller should attempt 3 reads to handle this condition before moving on.
   c. If the Block read has started (that is, the address is ACK'ed) then the entire read will complete successfully, and Intel® Xeon® Processor D-1500 Product Family will update the data only after the SMBus read has completed.
6. System is going from S0 to S4/S5. The thermal monitoring FW is fully operational if the system is in S0/S1, so the following only applies to S4/S5.



a. When Intel® Xeon® Processor D-1500 Product Family detects the OS request to go to S4/S5, it will take the SMLink0 controller offline as part of the system preparation. The external controller will see a period where its transactions are getting NACK'ed, and then see SLP_S3# assert.
This period is relatively short (a couple of seconds depending on how long all the devices take to place themselves into the D3 state), and would be far less than the 30 second limit mentioned above.

7. TEMP_ALERT# – Since there can be an internal reset, the TEMP_ALERT# may get asserted after the reset. The external controller must accept this assertion and handle it.

3.21.3.8.1 Example Algorithm for Handling Transaction

One algorithm for the transaction handling could be summarized as follows. This is just an example to illustrate the above rules. There could be other algorithms that can achieve the same results.

1. Perform SMBus transaction.
2. If ACK, then continue
3. If NACK
   a. Try again for 2 more times, in case Intel® Xeon® Processor D-1500 Product Family is busy updating data.
   b. If 3 successive transactions receive NACK, then
      - Ramp fans, assuming some general long reset or failure
      - Try every 1-10 seconds to see if SMBus transactions are now working
      - f they start then return to step 1
      - If they continue to fail, then stay in this step and poll, but keep the fans ramped up or implement some other failure recovery mechanism.

3.22 Intel® Management Engine (Intel® ME) and Intel® Management Engine Firmware (Intel® ME FW) 9.0

Key properties of Intel® Management Engine (Intel® ME):

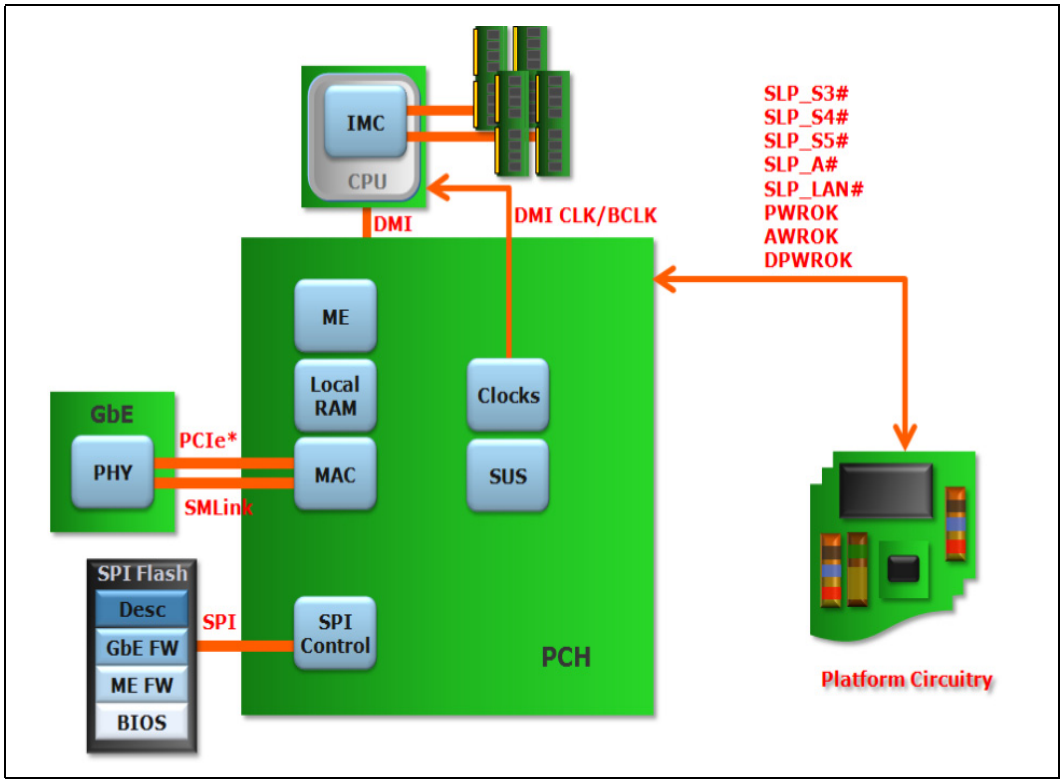
- Connectivity
  - — Integration into I/O subsystem of Intel® Xeon® Processor D-1500 Product Family
  - — Delivery of advanced I/O functions
- Security
  - — More secure (Intel root of trust) & isolated execution
  - — Increased security of flash file system
- Modularity & Partitioning
  - — OSV, VMM & SW Independence
  - — Rapid response to competitive changes
- Power
  - — Always On Always Connected

— Advanced functions in low power S4-S5 operation

— OS independent PM & thermal heuristics

Intel® ME FW provides a variety of services that range from low-level hardware initialization and provisioning to high-level end-user software based IT manageability services.

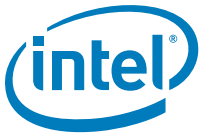
Figure 3-11. Intel® Xeon® Processor D-1500 Product Family Intel® Management Engine (Intel® ME) High-Level Block Diagram



3.22.1 Intel® ME Requirements

The following list of components compose the Intel ME hardware infrastructure:

- The Intel® ME is the general purpose controller that resides in Intel® Xeon® Processor D-1500 Product Family. It operates in parallel to, and is resource-isolated from, the host processor.
- The SPI flash device stores Intel ME Firmware code that is executed by the Intel® ME for its operations. Intel® Xeon® Processor D-1500 Product Family controls the flash device through the SPI interface and internal logic.
- In the M0 power state, the Intel® ME FW code is loaded from SPI flash into DRAM and cached in secure and isolated SRAM. In order to interface with DRAM, the Intel® ME utilizes the integrated memory controller (IMC). Communication between the IMC and the Intel® ME occurs in only M0 power state. In the lower Intel® ME power state, M3, code is executed exclusively from secure and isolated Intel® ME local RAM.



- The LAN controller embedded in Intel® Xeon® Processor D-1500 Product Family as well as the Intel Gigabit Platform LAN Connect device are required for Intel® ME.
- BIOS provides asset detection and POST diagnostics.

3.23 Serial Peripheral Interface (SPI)

The Serial Peripheral Interface (SPI) is a 4-pin interface that provides a lower-cost alternative for system flash versus the Firmware Hub on the LPC bus.

The 4-pin SPI interface consists of clock (CLK), master data out (Master Out Slave In (MOSI)), master data in (Master In Slave Out (MISO)) and an active low chip select (SPI_CS[1:0]#). SPI also adds 2 extra pins SPI_IO2 and SPI_IO3 for Quad I/O operation.

Intel® Xeon® Processor D-1500 Product Family supports up to two SPI flash devices using two separate Chip Select pins. Each SPI flash device can be up to 16 MB. Intel® Xeon® Processor D-1500 Product Family SPI interface supports 20 MHz, 33 MHz, and 50 MHz SPI devices. A SPI Flash device on with Chip Select 0 with a valid descriptor MUST be attached directly to Intel® Xeon® Processor D-1500 Product Family.

Note: When operating at 50 MHz, because of the 40% duty cycle Intel® Xeon® Processor D-1500 Product Family must use by dividing down from a 125 MHz clock, Intel® Xeon® Processor D-1500 Product Family SPI Flash Controller cannot meet the minimum high timing requirements of a 50 MHz SPI Flash component and a 66 MHz rated or faster SPI Flash component must be used.

Intel® Xeon® Processor D-1500 Product Family supports fast read which consist of:

1. Dual Output Fast Read (Single Input Dual Output)
2. Dual I/O Fast Read (Dual Input Dual Output)
3. Quad Output Fast Read (Single Input Quad Output)
4. Quad I/O Fast Read (Quad Input Quad Output)

Fast Read function will be enabled if the particular SPI part supports one of the function mentioned above along with support for SFDP (Serial Flash Discoverable Parameter).

Intel® Xeon® Processor D-1500 Product Family adds support for SFDP. SFDP is a JEDEC* standard that provides consistent method for describing functional and feature capabilities of serial flash devices in a standard set of internal parameter table. Intel® Xeon® Processor D-1500 Product Family SPI controller reads the internal parameter table and enables divergent features of multiple SPI vendor parts.

Intel® Xeon® Processor D-1500 Product Family adds third chip select SPI_CS2# for TPM support over SPI. TPM Bus will use SPI_CLK, SPI_MISO, SPI_MOSI and SPI_CS2# SPI signals.

Note: Communication on the SPI bus is done with a Master – Slave protocol. The Slave is connected to Intel® Xeon® Processor D-1500 Product Family and is implemented as a tri-state bus.If Boot BIOS Strap =’00’ then LPC is selected as the location for BIOS. BIOS may still be placed on LPC, but all platforms with Intel® Xeon® Processor D-1500 Product Family require a SPI flash connected directly to Intel® Xeon® Processor D-1500 Product Family's SPI bus with a valid descriptor connected to Chip Select 0 in order to boot.

Note: When SPI is selected by the Boot BIOS Destination Strap and a SPI device is detected by Intel® Xeon® Processor D-1500 Product Family, LPC based BIOS flash is disabled.

3.23.1 SPI Supported Feature Overview

SPI Flash on Intel® Xeon® Processor D-1500 Product Family has two operational modes, descriptor and non-descriptor.

3.23.1.1 Non-Descriptor Mode

Non-Descriptor Mode is not supported as a valid flash descriptor is required for all Intel® Xeon® Processor D-1500 Product Family Platforms.

3.23.1.2 Descriptor Mode

Descriptor Mode is required. It enables many features of the chipset:

- Integrated Gigabit Ethernet and Host processor for Gigabit Ethernet Software
- Intel Management Engine Firmware
- PCI Express* root port configuration
- Supports up to two SPI components using two separate chip select pins
- Hardware enforced security restricting master accesses to different regions
- Chipset Soft Strap regions provides the ability to use Flash NVM as an alternative to hardware pull-up/pull-down resistors for Intel® Xeon® Processor D-1500 Product Family and processor
- Supports the SPI Fast Read instruction and frequencies of up to 50 MHz
- Support Single Input, Dual Output Fast read
- Uses standardized Flash Instruction Set

3.23.1.2.1 SPI Flash Regions

In Descriptor Mode the Flash is divided into five separate regions:

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

Only three masters can access the four regions: Host processor running BIOS code, Integrated Gigabit Ethernet and Host processor running Gigabit Ethernet Software, and Intel® Management Engine. The Flash Descriptor is in Region 0 and it must be located in the first sector of Device 0 (Offset 0).

Flash Region Sizes

SPI flash space requirements differ by platform and configuration. The Flash Descriptor requires one 4 KB or larger block. GbE requires two 4 KB or larger blocks. The amount of flash space consumed is dependent on the erase granularity of the flash part and the platform requirements for the Intel® ME and BIOS regions.

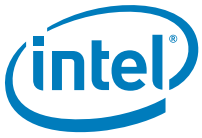


Table 3-51. Region Size versus Erase Granularity of Flash Components

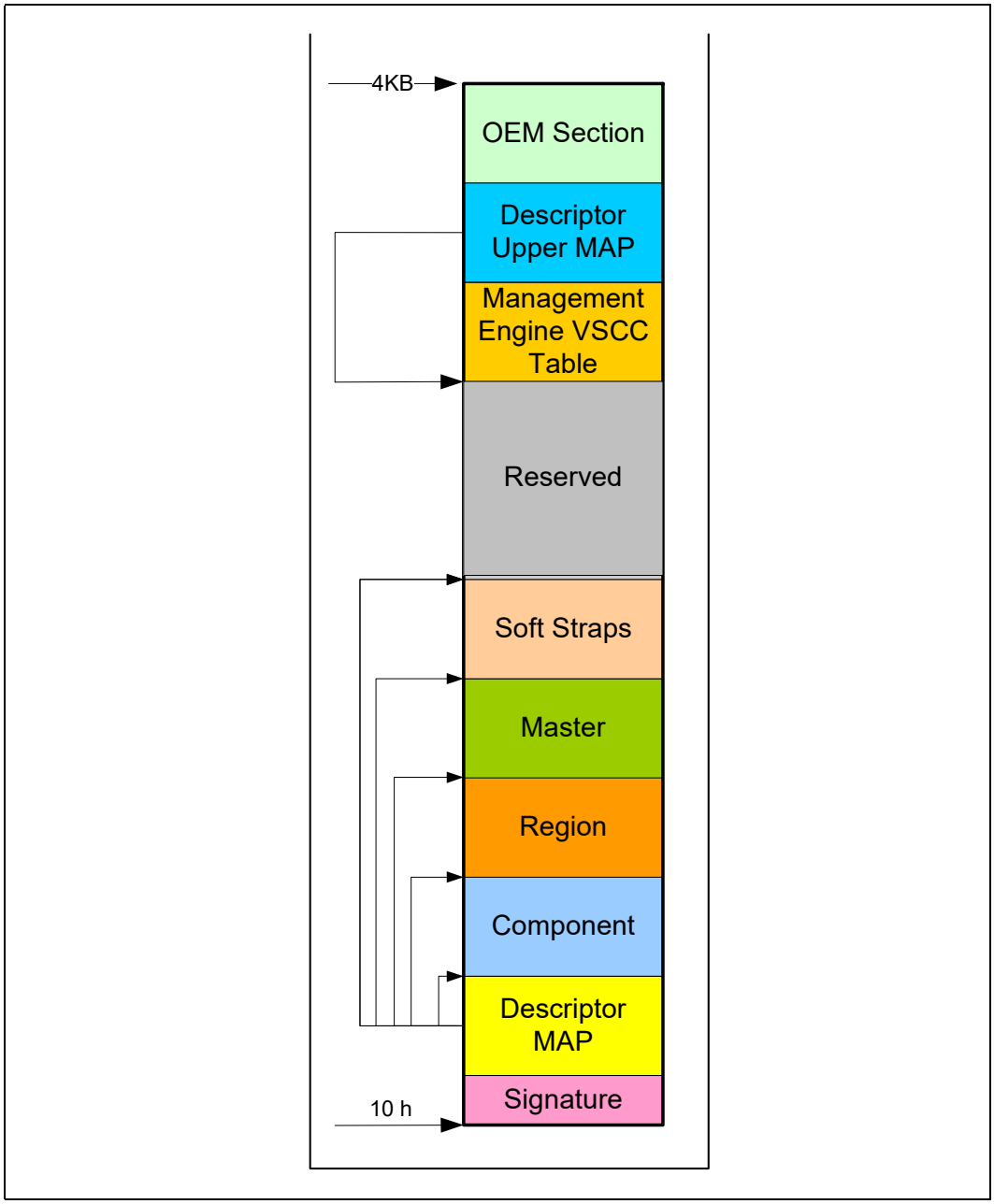
Region	Size with 4 KB Blocks	Size with 8 KB Blocks	Size with 64 KB Blocks
Descriptor	4 KB	8 KB	64 KB
GbE	8 KB	16 KB	128 KB
BIOS	Varies by Platform	Varies by Platform	Varies by Platform
Intel ME	Varies by Platform	Varies by Platform	Varies by Platform

3.23.2 Flash Descriptor

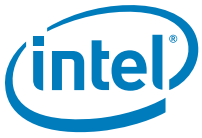
The maximum size of the Flash Descriptor is 4 KB. If the block/sector size of the SPI flash device is greater than 4 KB, the flash descriptor will only use the first 4 KB of the first block. The flash descriptor requires its own block at the bottom of memory (00h). The information stored in the Flash Descriptor can only be written during the manufacturing process as its read/write permissions must be set to Read only when the computer leaves the manufacturing floor.

The Flash Descriptor is made up of eleven sections (see Figure 3-12).

Figure 3-12. Flash Descriptor Sections



1. The Flash signature selects Descriptor Mode as well as verifies if the flash is programmed and functioning. The data at the bottom of the flash (offset 10h) must be 0FF0A55Ah in order to be in Descriptor mode.
2. The Descriptor map has pointers to the other five descriptor sections as well as the size of each.
3. The component section has information about the SPI flash in the system including: the number of components, density of each, illegal instructions (such as chip erase), and frequencies for read, fast read and write/erase instructions.



4. The Region section points to the three other regions as well as the size of each region.
5. The master region contains the security settings for the flash, granting read/write permissions for each region and identifying each master by a requestor ID. See Section 3.23.2.1 for more information.
6. The processor and Intel® Xeon® Processor D-1500 Product Family soft strap sections contain processor and Intel® Xeon® Processor D-1500 Product Family configurable parameters.
7. (same as 6) The processor and Intel® Xeon® Processor D-1500 Product Family soft strap sections contain processor and Intel® Xeon® Processor D-1500 Product Family configurable parameters.
8. The Reserved region between the top of the processor strap section and the bottom of the OEM Section is reserved for future chipset usages.
9. The Descriptor Upper MAP determines the length and base address of the Management Engine VSCC Table.
10. The Management Engine VSCC Table holds the JEDEC ID and the VSCC information of the entire SPI Flash supported by the NVM image.
11. OEM Section is 256 Bytes reserved at the top of the Flash Descriptor for use by OEM.

3.23.2.1 Descriptor Master Region

The master region defines read and write access setting for each region of the SPI device. The master region recognizes three masters: BIOS, Gigabit Ethernet, and Management Engine. Each master is only allowed to do direct reads of its primary regions.

Table 3-52. Region Access Control Table

Master Read/Write Access			
Region	**Processor and BIOS**	**Intel® ME**	**GbE Controller**
Descriptor	N/A	N/A	N/A
BIOS	Processor and BIOS can always read from and write to BIOS Region	Read / Write	Read / Write
Management Engine	Read / Write	Intel® ME can always read from and write to Intel ME Region	Read / Write
Gigabit Ethernet	Read / Write	Read / Write	GbE software can always read from and write to GbE region
Platform Data Region	N/A	N/A	N/A

3.23.3 Flash Access

There are two types of flash accesses:

Direct Access:

- Masters are allowed to do direct read only of their primary region

  - Gigabit Ethernet region can only be directly accessed by the Gigabit Ethernet controller. Gigabit Ethernet software must use Program Registers to access the Gigabit Ethernet region.
- Master's Host or Management Engine virtual read address is converted into the SPI Flash Linear Address (FLA) using the Flash Descriptor Region Base/Limit registers

Program Register Access:

- Program Register Accesses are not allowed to cross a 4 KB boundary and can not issue a command that might extend across two components
- Software programs the FLA corresponding to the region desired
  - Software must read the devices Primary Region Base/Limit address to create a FLA.

3.23.3.1 Direct Access Security

- Requester ID of the device must match that of the primary Requester ID in the Master Section
- Calculated Flash Linear Address must fall between primary region base/limit
- Direct Write not allowed
- Direct Read Cache contents are reset to 0's on a read from a different master
  - Supports the same cache flush mechanism in ICH7 which includes Program Register Writes

3.23.3.2 Register Access Security

- Only primary region masters can access the registers

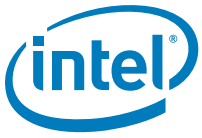
Note: Processor running Gigabit Ethernet software can access Gigabit Ethernet registers

- Masters are only allowed to read or write those regions they have read/write permission
- Using the Flash Region Access Permissions, one master can give another master read/write permissions to their area
- Using the five Protected Range registers, each master can add separate read/write protection above that granted in the Flash Descriptor for their own accesses
  - Example: BIOS may want to protect different regions of BIOS from being erased
  - Ranges can extend across region boundaries

3.23.4 Serial Flash Device Compatibility Requirements

A variety of serial flash devices exist in the market. For a serial flash device to be compatible with Intel® Xeon® Processor D-1500 Product Family SPI bus, it must meet the minimum requirements detailed in the following sections.

Note: All Intel® Xeon® Processor D-1500 Product Family platforms require Intel Management Engine Firmware.



3.23.4.1 Intel® Xeon® Processor D-1500 Product Family SPI Based BIOS Requirements

A serial flash device must meet the following minimum requirements when used explicitly for system BIOS storage.

- Erase size capability of at least one of the following: 64 Kbytes, 8 Kbytes, 4 Kbytes, or 256 bytes.
- Device must support multiple writes to a page without requiring a preceding erase cycle (Refer to Section 3.23.5)
- Serial flash device must ignore the upper address bits such that an address of FFFFFFh aliases to the top of the flash memory.
- SPI Compatible Mode 0 support (clock phase is 0 and data is latched on the rising edge of the clock).
- If the device receives a command that is not supported or incomplete (less than 8 bits), the device must complete the cycle gracefully without any impact on the flash content.
- An erase command (page, sector, block, chip, and so on) must set all bits inside the designated area (page, sector, block, chip, and so on) to 1 (Fh).
- Status Register bit 0 must be set to 1 when a write, erase or write to status register is in progress and cleared to 0 when a write or erase is NOT in progress.
- Devices requiring the Write Enable command must automatically clear the Write Enable Latch at the end of Data Program instructions.
- Byte write must be supported. The flexibility to perform a write between 1 byte to 64 bytes is recommended.
- Hardware Sequencing requirements are optional in BIOS only platforms.
- SPI flash parts that do not meet Hardware sequencing command set requirements may work in BIOS only platforms using software sequencing.

3.23.4.2 Integrated LAN Firmware SPI Flash Requirements

A serial flash device that will be used for system BIOS and Integrated LAN or Integrated LAN only must meet all the SPI Based BIOS Requirements plus:

- Hardware sequencing
- 4, 8, or 64 KB erase capability must be supported.

3.23.4.2.1 SPI Flash Unlocking Requirements for Integrated LAN

BIOS must ensure there is no SPI flash based read/write/erase protection on the GbE region. GbE firmware and drivers for the integrated LAN need to be able to read, write and erase the GbE region at all times.

3.23.4.3 Intel® Management Engine Firmware (Intel® ME FW) SPI Flash Requirements

Intel Management Engine Firmware must meet the SPI flash based BIOS Requirements plus:

- Hardware Sequencing.

- Flash part must be uniform 4-KB erasable block throughout the entire device or have 64 KB blocks with the first block (lowest address) divided into 4-KB or 8-KB blocks.
- Write protection scheme must meet SPI flash unlocking requirements for Intel ME.

3.23.4.3.1 SPI Flash Unlocking Requirements for Intel® Management Engine (Intel® ME)

Flash devices must be globally unlocked (read, write and erase access on the ME region) from power on by writing 00h to the flash's status register to disable write protection.

If the status register must be unprotected, it must use the enable write status register command 50h or write enable 06h.

Opcode 01h (write to status register) must then be used to write a single byte of 00h into the status register. This must unlock the entire part. If the SPI flash's status register has non-volatile bits that must be written to, bits [5:2] of the flash's status register must be all 0h to indicate that the flash is unlocked.

If bits [5:2] return a non zero values, the Intel® ME firmware will send a write of 00h to the status register. This must keep the flash part unlocked.

If there is no need to execute a write enable on the status register, then opcodes 06h and 50h must be ignored.

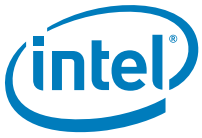
After global unlock, BIOS has the ability to lock down small sections of the flash as long as they do not involve the Intel® ME or GbE region.

3.23.4.4 Hardware Sequencing Requirements

Table 3-53 contains a list of commands and the associated opcodes that a SPI-based serial flash device must support in order to be compatible with hardware sequencing.

Table 3-53. Hardware Sequencing Commands and Opcode Requirements

Commands	Opcode	Notes
Write to Status Register	01h	Writes a byte to SPI flash's status register. Enable Write to Status Register command must be run prior to this command.
Program Data	02h	Single byte or 64 byte write as determined by flash part capabilities and software.
Read Data	03h	
Write Disable	04h	
Read Status	05h	Outputs contents of SPI flash's status register
Write Enable	06h	
Fast Read	0Bh	
Enable Write to Status Register	50h or 60h	Enables a bit in the status register to allow an update to the status register
Erase	Programmable	256B, 4 Kbyte, 8 Kbyte or 64 Kbyte
Full Chip Erase	C7h	
JEDEC ID	9Fh	See Section 3.23.4.4.3.



3.23.4.4.1 Single Input, Dual Output Fast Read

Intel® Xeon® Processor D-1500 Product Family now supports the functionality of a single input, dual output fast read. Opcode and address phase are shifted in serially to the serial flash SI (Serial In) pin. Data is read out after 8 clocks (dummy bits or wait states) from the both the SI and SO pin effectively doubling the through put of each fast read output. In order to enable this functionality, both Single Input Dual Output Fast Read Supported and Fast Read supported must be enabled

3.23.4.4.2 Serial Flash Discoverable Parameters (SFDP)

As the number of features keeps growing in the serial flash, the need for correct, accurate configuration increases. A method of determining configuration information is Serial Flash Discoverable Parameters (SFDP). Information such as VSCC values and flash attributes can be read directly from the flash parts. The discoverable parameter read opcode behaves like a fast read command. The opcode is 5Ah and the address cycle is 24 bits long. After the opcode 5Ah and address are clocked in, there will then be eight clocks (8 wait states) before valid data is clocked out. SFDP is a capability of the flash part, confirm with target flash vendor to see if it is supported.

In order for BIOS to take advantage of the 5Ah opcode it needs to be programmed in the Software sequencing registers.

3.23.4.4.3 JEDEC ID

Since each serial flash device may have unique capabilities and commands, the JEDEC ID is the necessary mechanism for identifying the device so the uniqueness of the device can be comprehended by the controller (master). The JEDEC ID uses the opcode 9Fh and a specified implementation and usage model. This JEDEC Standard Manufacturer and Device ID read method is defined in Standard JESD21-C, PRN03-NV.

3.23.5 Multiple Page Write Usage Model

The system BIOS and Intel Management Engine firmware usage models require that the serial flash device support multiple writes to a page (minimum of 512 writes) without requiring a preceding erase command. BIOS commonly uses capabilities such as counters that are used for error logging and system boot progress logging. These counters are typically implemented by using byte-writes to ‘increment’ the bits within a page that have been designated as the counter. The Intel ME firmware usage model requires the capability for multiple data updates within any given page. These data updates occur using byte-writes without executing a preceding erase to the given page. Both the BIOS and Intel ME firmware multiple page write usage models apply to sequential and non-sequential data writes.

Note: This usage model requirement is based on any given bit only being written once from a ‘1’ to a ‘0’without requiring the preceding erase. An erase would be required to change bits back to the 1 state.

3.23.5.1 Soft Flash Protection

There are two types of flash protection that are not defined in the flash descriptor supported by Intel® Xeon® Processor D-1500 Product Family:

1. BIOS Range Write Protection
2. SMI#-Based Global Write Protection

Both mechanisms are logically OR'd together such that if any of the mechanisms indicate that the access should be blocked, then it is blocked. Table 3-54 provides a summary of the mechanisms.

Table 3-54. Flash Protection Mechanism Summary

Mechanism	Accesses Blocked	Range Specific?	Reset-Override or SMI#-Override?	Equivalent Function on FWH
BIOS Range Write Protection	Writes	Yes	Reset Override	FWH Sector Protection
Write Protect	Writes	No	SMI# Override	Same as Write Protect in Intel® ICHs for FWH

A blocked command will appear to software to finish, except that the Blocked Access status bit is set in this case.

3.23.5.2 BIOS Range Write Protection

Intel® Xeon® Processor D-1500 Product Family provides a method for blocking writes to specific ranges in the SPI flash when the Protected BIOS Ranges are enabled. This is achieved by checking the Opcode type information (which can be locked down by the initial Boot BIOS) and the address of the requested command against the base and limit fields of a Write Protected BIOS range.

Note: Once BIOS has locked down the Protected BIOS Range registers, this mechanism remains in place until the next system reset.

3.23.5.3 SMI# Based Global Write Protection

Intel® Xeon® Processor D-1500 Product Family provides a method for blocking writes to the SPI flash when the Write Protected bit is cleared (that is, protected). This is achieved by checking the Opcode type information (which can be locked down by the initial Boot BIOS) of the requested command.

The Write Protect and Lock Enable bits interact in the same manner for SPI BIOS as they do for the FWH BIOS.

3.23.6 Flash Device Configurations

Intel® Xeon® Processor D-1500 Product Family-based platform must have a SPI flash connected directly to Intel® Xeon® Processor D-1500 Product Family with a valid descriptor and Intel Management Engine Firmware. BIOS may be stored in other locations such as Firmware Hub and SPI flash hooked up directly to an embedded controller. Note this will not avoid the direct SPI flash connected to Intel® Xeon® Processor D-1500 Product Family requirement.

3.23.7 SPI Flash Device Recommended Pinout

Table 3-55 contains the recommended serial flash device pin-out for an 8-pin device. Use of the recommended pin-out on an 8-pin device reduces complexities involved with designing the serial flash device onto a motherboard and allows for support of a common footprint usage model (refer to Section 3.23.8.1).

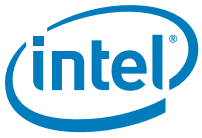


Table 3-55. Recommended Pinout for 8-Pin Serial Flash Device

Pin #	Signal
1	Chips Select
2	Data Output
3	Write Protect
4	Ground
5	Data Input
6	Serial Clock
7	Hold / Reset
8	Supply Voltage

Although an 8-pin device is preferred over a 16-pin device due to footprint compatibility, the following table contains the recommended serial flash device pin-out for a 16-pin SOIC.

3.23.8 Serial Flash Device Package

Table 3-56. Recommended Pinout for 16-Pin Serial Flash Device

Pin #	Signal	Pin #	Signal
1	Hold / Reset	9	Write Protect
2	Supply Voltage	10	Ground
3	No Connect	11	No Connect
4	No Connect	12	No Connect
5	No Connect	13	No Connect
6	No Connect	14	No Connect
7	Chip Select	15	Serial Data In
8	Serial Data Out	16	Serial Clock

3.23.8.1 Common Footprint Usage Model

In order to minimize platform motherboard redesign and to enable platform Bill of Material (BOM) selectability, many PC System OEMs design their motherboard with a single common footprint. This common footprint allows population of a soldered down device or a socket that accepts a leadless device. This enables the board manufacturer to support, using selection of the appropriate BOM, either of these solutions on the same system without requiring any board redesign.

The common footprint usage model is desirable during system debug and by flash content developers since the leadless device can be easily removed and reprogrammed without damage to device leads. When the board and flash content is mature for high-volume production, both the socketed leadless solution and the soldered down leaded solution are available through BOM selection.

3.23.8.2 Serial Flash Device Package Recommendations

It is highly recommended that the common footprint usage model be supported. An example of how this can be accomplished is as follows:

- The recommended pinout for 8-pin serial flash devices is used (see Section 3.23.7).

- The 8-pin device is supported in either an 8-contact VDFPN (6x5 mm MLP) package or an 8-contact WSON (5x6 mm) package. These packages can fit into a socket that is land pattern compatible with the wide body SO8 package.
- The 8-pin device is supported in the SO8 (150 mil) and in the wide-body SO8 (200 mil) packages.

The 16-pin device is supported in the SO16 (300 mil) package.

3.23.9 PWM Outputs

This signal is driven as open-drain. An external pull-up resistor is integrated into the fan to provide the rising edge of the PWM output signal. The PWM output is driven low during reset, which represents 0% duty cycle to the fans. After reset de-assertion, the PWM output will continue to be driven low until one of the following occurs:

- The internal PWM control register is programmed to a non-zero value by appropriate firmware.
- The watchdog timer expires (enabled and set at 4 seconds by default).
- The polarity of the signal is inverted by firmware.

If a PWM output will be programmed to inverted polarity for a particular fan, then the low voltage driven during reset represents 100% duty cycle to the fan.

3.23.10 TACH Inputs

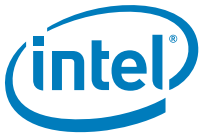
This signal is driven as an open-collector or open-drain output from the fan. An external pull-up is expected to be implemented on the motherboard to provide the rising edge of the TACH input. This signal has analog hysteresis and digital filtering due to the potentially slow rise and fall times. This signal has a weak internal pull-up resistor to keep the input buffer from floating if the TACH input is not connected to a fan.

3.24 Feature Capability Mechanism

A set of registers is included in Intel® Xeon® Processor D-1500 Product Family LPC Interface (Device 31, Function 0, offset E0h–EBh) that allows the system software or BIOS to easily determine the features supported by Intel® Xeon® Processor D-1500 Product Family. These registers can be accessed through LPC PCI configuration space, thus allowing for convenient single point access mechanism for chipset feature detection.

This set of registers consists of:

- Capability ID (FDCAP)
- Capability Length (FDLEN)
- Capability Version and Vendor-Specific Capability ID (FDVER)
- Feature Vector (FVECT)



3.25 Intel® Virtualization Technology (Intel® VT)

Intel® Virtualization Technology (Intel® VT) makes a single system appear as multiple independent systems to software. This allows for multiple, independent operating systems to be running simultaneously on a single system. Intel® VT comprises technology components to support virtualization of platforms based on Intel architecture microprocessors and chipsets. The first revision of this technology (Intel® VT-x) added hardware support in the processor to improve the virtualization performance and robustness. The second revision of this specification (Intel® VT-d) adds chipset hardware implementation to improve I/O performance and robustness.

The Intel® VT-d specification and other VT documents can be referenced here: http://www.intel.com/technology/platform-technology/virtualization/index.htm

3.25.1 Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d) Objectives

The key Intel® VT-d objectives are domain based isolation and hardware based virtualization. A domain can be abstractly defined as an isolated environment in a platform to which a subset of host physical memory is allocated. Virtualization allows for the creation of one or more partitions on a single system. This could be multiple partitions in the same OS or there can be multiple operating system instances running on the same system offering benefits such as system consolidation, legacy migration, activity partitioning or security.

3.25.2 Intel® VT-d Features Supported

- The following devices and functions support FLR in Intel® Xeon® Processor D-1500 Product Family:
  - SATA Host Controller 1 (Device 31: Function 2)
  - SATA Host Controller 2 (Device 31: Function 5)
  - USB2 (EHCI) Host Controller 1 (Device 29: Function 0)
  - GbE Lan Host Controller (Device 25: Function 0)
- Interrupt virtualization support for IOxAPIC
- Virtualization support for HPETs

3.25.3 Support for Function Level Reset (FLR) in Intel® Xeon® Processor D-1500 Product Family

Intel® VT-d allows system software (VMM/OS) to assign I/O devices to multiple domains. The system software, then, requires ways to reset I/O devices or their functions within, as it assigns/re-assigns I/O devices from one domain to another. The reset capability is required to ensure the devices have undergone proper re-initialization and are not keeping the stale state. A standard ability to reset I/O devices is also useful for the VMM in case where a guest domain with assigned devices has become unresponsive or has crashed.

PCI Express defines a form of device hot reset which can be initiated through the Bridge Control register of the root/switch port to which the device is attached. However, the hot reset cannot be applied selectively to specific device functions. Also, no similar standard functionality exists for resetting root-complex integrated devices.

Current reset limitations can be addressed through a *function level reset* (FLR) mechanism that allows software to independently reset specific device functions.

3.25.4 Virtualization Support for Intel® Xeon® Processor D-1500 Product Family IOxAPIC

The Intel® VT-d architecture extension requires Interrupt Messages to go through the similar Address Remapping as any other memory requests. This is to allow domain isolation for interrupts such that a device assigned in one domain is not allowed to generate interrupts to another domain.

The Address Remapping for Intel® VT-d is based on the Bus:Device:Function field associated with the requests. Hence, it is required for the internal IOxAPIC to initiate the Interrupt Messages using a unique Bus:Device:Function.

Intel® Xeon® Processor D-1500 Product Family supports BIOS programmable unique Bus:Device:Function for the internal IOxAPIC. The Bus:Device:Function field does not change the IOxAPIC functionality in anyway, nor promoting IOxAPIC as a stand-alone device. The field is only used by the IOxAPIC in the following:

- As the Requestor ID when initiating Interrupt Messages to the processor
- As the Completer ID when responding to the reads targeting the IOxAPIC's Memory-Mapped I/O registers

3.25.5 Virtualization Support for High Precision Event Timer (HPET)

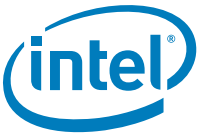
The Intel® VT-d architecture extension requires Interrupt Messages to go through the similar Address Remapping as any other memory requests. This is to allow domain isolation for interrupts such that a device assigned in one domain is not allowed to generate interrupts to another domain.

The Address Remapping for Intel® VT-d is based on the Bus:Device:Function field associated with the requests. Hence, it is required for the HPET to initiate the direct FSB Interrupt Messages using unique Bus:Device:Function.

Intel® Xeon® Processor D-1500 Product Family supports BIOS programmable unique Bus:Device:Function for each of the HPET timers. The Bus:Device:Function field does not change the HPET functionality in anyway, nor promoting it as a stand-alone device. The field is only used by the HPET timer in the following:

- As the Requestor ID when initiating direct interrupt messages to the processor
- As the Completer ID when responding to the reads targeting its Memory-Mapped registers
- The registers for the programmable Bus:Device:Function for HPET timer 7:0 reside under the D31:F0 LPC Bridge's configuration space.

§



4 Register and Memory Mapping

Intel® Xeon® Processor D-1500 Product Family contains registers that are located in the processor I/O space and memory space and sets of PCI configuration registers that are located in PCI configuration space. This chapter describes Intel® Xeon® Processor D-1500 Product Family I/O and memory maps at the register-set level. Register access is also described. Register-level address maps and Individual register bit descriptions are provided in the following chapters. The following notations and definitions are used in the register/instruction description chapters.

Note: All Chipset Registers are located in the core well unless otherwise indicated.

RO	Read Only. In some cases, if a register is read only, writes to this register location have no effect. However, in other cases, two separate registers are located at the same location where a read accesses one of the registers and a write accesses the other register. See the I/O and memory map tables for details.
WO	Write Only. In some cases, if a register is write only, reads to this register location have no effect. However, in other cases, two separate registers are located at the same location where a read accesses one of the registers and a write accesses the other register. See the I/O and memory map tables for details.
R/W	Read/Write. A register with this attribute can be read and written.
R/WC	Read/Write Clear. A register bit with this attribute can be read and written. However, a write of 1 clears (sets to 0) the corresponding bit and a write of 0 has no effect.
R/WO	Read/Write-Once. A register bit with this attribute can be written only once after power up. After the first write, the bit becomes read only.
R/WL	Read/Write Lockable. A register bit with the attribute can be read at any time but writes may only occur if the associated lock bit is set to unlock. If the associated lock bit is set to lock, this register bit becomes RO unless otherwise indicated.
R/WLO	Read/Write, Lock-Once. A register bit with this attribute can be written to the non-locked value multiple times, but to the locked value only once. After the locked value has been written, the bit becomes read only.
R/W/SN	Read/Write register initial value loaded from NVM.
Reserved	The value of reserved bits must never be changed. For details see Section 4.2.
Default	When Intel® Xeon® Processor D-1500 Product Family is reset, it sets its registers to predetermined default states. It is the responsibility of the system initialization software to determine configuration, operating parameters, and optional system features that are applicable, and to program Intel® Xeon® Processor D-1500 Product Family registers accordingly.

Bold Register bits that are highlighted in bold text indicate that the bit is implemented in Intel® Xeon® Processor D-1500 Product Family. Register bits that are not implemented or are hardwired will remain in plain text.

4.1 PCI Devices and Functions

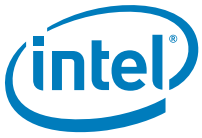
Intel® Xeon® Processor D-1500 Product Family incorporates a variety of PCI devices and functions, as shown in Table 4-1.

Device Functions can individually be disabled. The integrated Gigabit Ethernet controller will be disabled if no Platform LAN Connect component is detected (See Section 3.3). When a function is disabled, it does not appear at all to the software. A disabled function will not respond to any register reads or writes, insuring that these devices appear hidden to software.

Table 4-1. PCI Devices and Functions

Bus:Device:Function	Function Description
Bus 0:Device 31:Function 0	LPC Controller[1]
Bus 0:Device 31:Function 2	**SATA Controller #1**
Bus 0:Device 31:Function 3	SMBus Controller
Bus 0:Device 31:Function 5	SATA Controller #2[2]
Bus 0:Device 31:Function 6	Thermal Subsystem
Bus 0:Device 29:Function 0[3]	USB EHCI Controller #1
Bus 0:Device 28:Function 0	PCI Express* Port 1
Bus 0:Device 28:Function 1	PCI Express Port 2
Bus 0:Device 28:Function 2	PCI Express Port 3
Bus 0:Device 28:Function 3	PCI Express Port 4
Bus 0:Device 28:Function 4	PCI Express Port 5
Bus 0:Device 28:Function 5	PCI Express Port 6
Bus 0:Device 28:Function 6	PCI Express Port 7
Bus 0:Device 28:Function 7	PCI Express Port 8
Bus 0:Device 25:Function 0	Gigabit Ethernet Controller
Bus 0:Device 22:Function 0	Intel® Management Engine Interface #1
Bus 0:Device 22:Function 1	Intel Management Engine Interface #2
Bus 0:Device 22:Function 2	IDE-R
Bus 0:Device 22:Function 3	KT
Bus 0:Device 20:Function 0	xHCI Controller

Notes:
1. The PCI-to-LPC bridge contains registers that control LPC, Power Management, System Management, GPIO, Processor Interface, RTC, Interrupts, Timers, and DMA.
2. SATA controller 2 (D31:F5) is only visible when D31:F2 CC.SCC=01h.
3. Prior to BIOS initialization of Intel® Xeon® Processor D-1500 Product Family USB subsystem, the EHCI controller will appear as Function 7. After BIOS initialization, the EHCI controllers will be Function 0.
4. This table shows the default PCI Express* Function Number-to-Root Port mapping. Function numbers for a given root port are assignable through the "Root Port Function Number and Hide for PCI Express Root Ports" register (RCBA+0404h).



4.2 PCI Configuration Map

Each PCI function on Intel® Xeon® Processor D-1500 Product Family has a set of PCI configuration registers. The register address map tables for these register sets are included at the beginning of the chapter for the particular function.

Configuration Space registers are accessed through configuration cycles on the PCI bus by the Host bridge using configuration mechanism #1 detailed in the *PCI Local Bus Specification, Revision 2.3*.

Some of the PCI registers contain reserved bits. Software must deal correctly with fields that are reserved. On reads, software must use appropriate masks to extract the defined bits and not rely on reserved bits being any particular value. On writes, software must ensure that the values of reserved bit positions are preserved. That is, the values of reserved bit positions must first be read, merged with the new values for other bit positions and then written back. The software does not need to perform read, merge, write operation for the configuration address register.

In addition to reserved bits within a register, the configuration space contains reserved locations. Software should not write to reserved PCI configuration locations in the device-specific region (above address offset 3Fh).

4.3 I/O Map

The I/O map is divided into Fixed and Variable address ranges. Fixed ranges cannot be moved, but in some cases can be disabled. Variable ranges can be moved and can also be disabled.

4.3.1 Fixed I/O Address Ranges

Table 4-2 shows the Fixed I/O decode ranges from the processor perspective. For each I/O range, there may be separate behavior for reads and writes. Internal message cycles that go to target ranges that are marked as "Reserved" will not be decoded by Intel® Xeon® Processor D-1500 Product Family, and will be passed to PCI, unless the Subtractive Decode Policy bit is set (D31:F0:Offset 42h, bit 0). If a PCI master targets one of the fixed I/O target ranges, it will be positively decoded by Intel® Xeon® Processor D-1500 Product Family in medium speed.

Address ranges that are not listed or marked "Reserved" are **not** decoded by Intel® Xeon® Processor D-1500 Product Family (unless assigned to one of the variable ranges).

Table 4-2. Fixed I/O Ranges Decoded by Intel® Xeon® Processor D-1500 Product Family (Sheet 1 of 3)

I/O Address	Read Target	Write Target	Internal Unit
00h–08h	DMA Controller	DMA Controller	DMA
09h–0Eh	RESERVED	DMA Controller	DMA
0Fh	DMA Controller	DMA Controller	DMA
10h–18h	DMA Controller	DMA Controller	DMA
19h–1Eh	RESERVED	DMA Controller	DMA
1Fh	DMA Controller	DMA Controller	DMA

Table 4-2. Fixed I/O Ranges Decoded by Intel® Xeon® Processor D-1500 Product Family (Sheet 2 of 3)

I/O Address	Read Target	Write Target	Internal Unit
20h–21h	Interrupt Controller	Interrupt Controller	Interrupt
24h–25h	Interrupt Controller	Interrupt Controller	Interrupt
28h–29h	Interrupt Controller	Interrupt Controller	Interrupt
2Ch–2Dh	Interrupt Controller	Interrupt Controller	Interrupt
2Eh–2Fh	LPC SIO	LPC SIO	Forwarded to LPC
30h–31h	Interrupt Controller	Interrupt Controller	Interrupt
34h–35h	Interrupt Controller	Interrupt Controller	Interrupt
38h–39h	Interrupt Controller	Interrupt Controller	Interrupt
3Ch–3Dh	Interrupt Controller	Interrupt Controller	Interrupt
40h–42h	Timer/Counter	Timer/Counter	PIT (8254)
43h	RESERVED	Timer/Counter	PIT
4Eh–4Fh	LPC SIO	LPC SIO	Forwarded to LPC
50h–52h	Timer/Counter	Timer/Counter	PIT
53h	RESERVED	Timer/Counter	PIT
60h	Microcontroller	Microcontroller	Forwarded to LPC
61h	NMI Controller	NMI Controller	Processor I/F
62h	Microcontroller	Microcontroller	Forwarded to LPC
64h	Microcontroller	Microcontroller	Forwarded to LPC
66h	Microcontroller	Microcontroller	Forwarded to LPC
70h	RESERVED[1]	NMI and RTC Controller	RTC
71h	RTC Controller	RTC Controller	RTC
72h	RTC Controller	NMI and RTC Controller	RTC
73h	RTC Controller	RTC Controller	RTC
74h	RTC Controller	NMI and RTC Controller	RTC
75h	RTC Controller	RTC Controller	RTC
76h	RTC Controller	NMI and RTC Controller	RTC
77h	RTC Controller	RTC Controller	RTC
80h	DMA Controller, LPC, PCI, or PCIe*	DMA Controller and LPC, PCI, or PCIe	DMA
81h–83h	DMA Controller	DMA Controller	DMA
84h–86h	DMA Controller	DMA Controller and LPC, PCI, or PCIe	DMA
87h	DMA Controller	DMA Controller	DMA
88h	DMA Controller	DMA Controller and LPC, PCI, or PCIe	DMA
89h–8Bh	DMA Controller	DMA Controller	DMA
8Ch–8Eh	DMA Controller	DMA Controller and LPC, PCI, or PCIe	DMA
8Fh	DMA Controller	DMA Controller	DMA
90h–91h	DMA Controller	DMA Controller	DMA
92h	Reset Generator	Reset Generator	Processor I/F
93h–9Fh	DMA Controller	DMA Controller	DMA
A0h–A1h	Interrupt Controller	Interrupt Controller	Interrupt
A4h–A5h	Interrupt Controller	Interrupt Controller	Interrupt
A8h–A9h	Interrupt Controller	Interrupt Controller	Interrupt
ACh–ADh	Interrupt Controller	Interrupt Controller	Interrupt
B0h–B1h	Interrupt Controller	Interrupt Controller	Interrupt

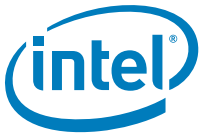


Table 4-2. Fixed I/O Ranges Decoded by Intel® Xeon® Processor D-1500 Product Family (Sheet 3 of 3)

I/O Address	Read Target	Write Target	Internal Unit
B2h–B3h	Power Management	Power Management	Power Management
B4h–B5h	Interrupt Controller	Interrupt Controller	Interrupt
B8h–B9h	Interrupt Controller	Interrupt Controller	Interrupt
BCh–BDh	Interrupt Controller	Interrupt Controller	Interrupt
C0h–D1h	DMA Controller	DMA Controller	DMA
D2h–DDh	RESERVED	DMA Controller	DMA
DEh–DFh	DMA Controller	DMA Controller	DMA
F0h	FERR# / Interrupt Controller	FERR# / Interrupt Controller	Processor I/F
170h–177h	SATA Controller, PCI, or PCIe	SATA Controller, PCI, or PCIe*	SATA
1F0h–1F7h	SATA Controller, PCI, or PCIe	SATA Controller, PCI, or PCIe	SATA
200h–207h	Gameport Low	Gameport Low	Forwarded to LPC
208h–20Fh	Gameport High	Gameport High	Forwarded to LPC
376h	SATA Controller, PCI, or PCIe	SATA Controller, PCI, or PCIe	SATA
3F6h	SATA Controller, PCI, or PCIe	SATA Controller, PCI, or PCIe	SATA
4D0h–4D1h	Interrupt Controller	Interrupt Controller	Interrupt
CF9h	Reset Generator	Reset Generator	Processor I/F

Note:
1. See Section 7.7.2.

4.3.2 Variable I/O Decode Ranges

Table 4-3 shows the Variable I/O Decode Ranges. They are set using Base Address Registers (BARs) or other configuration bits in the various PCI configuration spaces. The PNP software (PCI or ACPI) can use their configuration mechanisms to set and adjust these values.

Warning: The Variable I/O Ranges should not be set to conflict with the Fixed I/O Ranges. Unpredictable results if the configuration software allows conflicts to occur. Intel® Xeon® Processor D-1500 Product Family does not perform any checks for conflicts.

Table 4-3. Variable I/O Decode Ranges (Sheet 1 of 2)

Range Name	Mappable	Size (Bytes)	Target
ACPI	Anywhere in 64 KB I/O Space	64	Power Management
IDE Bus Master	Anywhere in 64 KB I/O Space	1. 16 or 32 2. 16	1. SATA Host Controller #1, #2 2. IDE-R
Native IDE Command	Anywhere in 64 KB I/O Space[1]	8	1. SATA Host Controller #1, #2 2. IDE-R
Native IDE Control	Anywhere in 64 KB I/O Space[1]	4	1. SATA Host Controller #1, #2 2. IDE-R
SATA Index/Data Pair	Anywhere in 64 KB I/O Space	16	SATA Host Controller #1, #2
SMBus	Anywhere in 64 KB I/O Space	32	SMB Unit
TCO	96 Bytes above ACPI Base	32	TCO Unit
GPIO	Anywhere in 64 KB I/O Space	128	GPIO Unit

Table 4-3. Variable I/O Decode Ranges (Sheet 2 of 2)

Range Name	Mappable	Size (Bytes)	Target
Parallel Port	3 Ranges in 64 KB I/O Space	8[3]	LPC Peripheral
Serial Port 1	8 Ranges in 64 KB I/O Space	8	LPC Peripheral
Serial Port 2	8 Ranges in 64 KB I/O Space	8	LPC Peripheral
Floppy Disk Controller	2 Ranges in 64 KB I/O Space	8	LPC Peripheral
LAN	Anywhere in 64 KB I/O Space	32[2]	LAN Unit
LPC Generic 1	Anywhere in 64 KB I/O Space	4 to 256	LPC Peripheral
LPC Generic 2	Anywhere in 64 KB I/O Space	4 to 256	LPC Peripheral
LPC Generic 3	Anywhere in 64 KB I/O Space	4 to 256	LPC Peripheral
LPC Generic 4	Anywhere in 64 KB I/O Space	4 to 256	LPC Peripheral
I/O Trapping Ranges	Anywhere in 64 KB I/O Space	1 to 256	Trap on Backbone
PCI Bridge	Anywhere in 64 KB I/O Space	I/O Base/ Limit	PCI Bridge
PCI Express* Root Ports	Anywhere in 64 KB I/O Space	I/O Base/ Limit	PCI Express Root Ports 1–8
KT	Anywhere in 64 KB I/O Space	8	KT

Notes:
1. All ranges are decoded directly from internal messages. The I/O cycles will not be seen on PCI, except the range associated with PCI bridge.
2. The LAN range is typically not used, as the registers can also be accessed using a memory space.
3. There is also an alias 400h above the parallel port range that is used for ECP parallel ports.

4.4 Memory Map

Table 4-4 shows (from the processor perspective) the memory ranges that Intel® Xeon® Processor D-1500 Product Family decodes. Cycles that arrive from internal messages that are not directed to any of the internal memory targets that decode directly from internal messages will be driven out on PCI unless the Subtractive Decode Policy bit is set (D31:F0:Offset 42h, bit 0).

PCI cycles generated by external PCI masters will be positively decoded unless they fall in the PCI-to-PCI bridge memory forwarding ranges (those addresses are reserved for PCI peer-to-peer traffic). If the cycle is not in the internal LAN controller's range, it will be forwarded up to the processing unit. Software must not attempt locks to Intel® Xeon® Processor D-1500 Product Family memory-mapped I/O ranges for EHCI and HPET. If attempted, the lock is not honored which means potential deadlock conditions may occur.

Table 4-4. Memory Decode Ranges from Processor Perspective (Sheet 1 of 3)

Memory Range	Target	Dependency/Comments
0000 0000h–000D FFFFh 0010 0000h–TOM (Top of Memory)	Main Memory	TOM registers in Host controller
000E 0000h–000E FFFFh	LPC or SPI	Bit 6 in BIOS Decode Enable register is set
000F 0000h–000F FFFFh	LPC or SPI	Bit 7 in BIOS Decode Enable register is set
FEC_ _000h–FEC_ _040h	I/O(x) APIC inside Intel® Xeon® Processor D-1500 Product Family	_ _is controlled using APIC Range Select (ASEL) field and APIC Enable (AEN) bit
FEC1 0000h–FEC1 7FFF	PCI Express* Port 1	PCI Express* Root Port 1 I/OxAPIC Enable (PAE) set

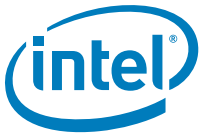


Table 4-4. Memory Decode Ranges from Processor Perspective (Sheet 2 of 3)

Memory Range	Target	Dependency/Comments
FEC1 8000h–FEC1 FFFFh	PCI Express* Port 2	PCI Express* Root Port 2 I/OxAPIC Enable (PAE) set
FEC2 0000h–FEC2 7FFFh	PCI Express* Port 3	PCI Express* Root Port 3 I/OxAPIC Enable (PAE) set
FEC2 8000h–FEC2 FFFFh	PCI Express* Port 4	PCI Express* Root Port 4 I/OxAPIC Enable (PAE) set
FEC3 0000h–FEC3 7FFFh	PCI Express* Port 5	PCI Express* Root Port 5 I/OxAPIC Enable (PAE) set
FEC3 8000h–FEC3 FFFFh	PCI Express* Port 6	PCI Express* Root Port 6 I/OxAPIC Enable (PAE) set
FEC4 0000h–FEC4 7FFF	PCI Express* Port 7	PCI Express* Root Port 7 I/OxAPIC Enable (PAE) set
FEC4 8000h–FEC4 FFFF	PCI Express* Port 8	PCI Express* Root Port 8 I/OxAPIC Enable (PAE) set
FFC0 0000h–FFC7 FFFFh FF80 0000h–FF87 FFFFh	LPC or SPI (or PCI)[2]	Bit 8 in BIOS Decode Enable register is set
FFC8 0000h–FFCF FFFFh FF88 0000h–FF8F FFFFh	LPC or SPI (or PCI)[2]	Bit 9 in BIOS Decode Enable register is set
FFD0 0000h–FFD7 FFFFh FF90 0000h–FF97 FFFFh	LPC or SPI (or PCI)[2]	Bit 10 in BIOS Decode Enable register is set
FFD8 0000h–FFDF FFFFh FF98 0000h–FF9F FFFFh	LPC or SPI (or PCI)[2]	Bit 11 in BIOS Decode Enable register is set
FFE0 000h–FFE7 FFFFh FFA0 0000h–FFA7 FFFFh	LPC or SPI (or PCI)[2]	Bit 12 in BIOS Decode Enable register is set
FFE8 0000h–FFEF FFFFh FFA8 0000h–FFAF FFFFh	LPC or SPI (or PCI)[2]	Bit 13 in BIOS Decode Enable register is set
FFF0 0000h–FFF7 FFFFh FFB0 0000h–FFB7 FFFFh	LPC or SPI (or PCI)[2]	Bit 14 in BIOS Decode Enable register is set
FFF8 0000h–FFFF FFFFh FFB8 0000h–FFBF FFFFh	LPC or SPI (or PCI)[2]	Always enabled. The top two 64 KB blocks of this range can be swapped, as described in Section 4.4.1.
FF70 0000h–FF7F FFFFh FF30 0000h–FF3F FFFFh	LPC or SPI (or PCI)[2]	Bit 3 in BIOS Decode Enable register is set
FF60 0000h–FF6F FFFFh FF20 0000h–FF2F FFFFh	LPC or SPI (or PCI)[2]	Bit 2 in BIOS Decode Enable register is set
FF50 0000h–FF5F FFFFh FF10 0000h–FF1F FFFFh	LPC or SPI (or PCI)[2]	Bit 1 in BIOS Decode Enable register is set
FF40 0000h–FF4F FFFFh FF00 0000h–FF0F FFFFh	LPC or SPI (or PCI)[2]	Bit 0 in BIOS Decode Enable register is set
128 KB anywhere in 4 GB range	Integrated LAN Controller	Enable using BAR in D25:F0 (Integrated LAN Controller MBARA)
4 KB anywhere in 4 GB range	Integrated LAN Controller	Enable using BAR in D25:F0 (Integrated LAN Controller MBARB)
1 KB anywhere in 4 GB range	USB EHCI Controller #1[1]	Enable using standard PCI mechanism (D29:F0)
64 KB anywhere in 4 GB range	USB xHCI Controller	Enable using standard PCI mechanism (D20:F0)
FED0 X000h–FED0 X3FFh	High Precision Event Timers[1]	BIOS determines the "fixed" location which is one of four, 1-KB ranges where X (in the first column) is 0h, 1h, 2h, or 3h.
FED4 0000h–FED4 FFFFh	TPM on LPC	None
Memory Base/Limit anywhere in 4 GB range	PCI Bridge	Enable using standard PCI mechanism (D30:F0)
Prefetchable Memory Base/Limit anywhere in 64-bit address range	PCI Bridge	Enable using standard PCI mechanism (D30:F0)
64 KB anywhere in 4 GB range	LPC	LPC Generic Memory Range. Enable using setting bit[0] of the LPC Generic Memory Range register (D31:F0:offset 98h).
32 Bytes anywhere in 64-bit address range	SMBus	Enable using standard PCI mechanism (D31:F3)

Table 4-4. Memory Decode Ranges from Processor Perspective (Sheet 3 of 3)

Memory Range	Target	Dependency/Comments
2 KB anywhere above 64 KB to 4 GB range	SATA Host Controller #1	AHCI memory-mapped registers. Enable using standard PCI mechanism (D31:F2)
Memory Base/Limit anywhere in 4 GB range	PCI Express* Root Ports 1-8	Enable using standard PCI mechanism (D28: F 0-7)
Prefetchable Memory Base/Limit anywhere in 64-bit address range	PCI Express Root Ports 1-8	Enable using standard PCI mechanism (D28:F 0-7)
4 KB anywhere in 64-bit address range	Thermal Reporting	Enable using standard PCI mechanism (D31:F6 TBAR/ TBARH)
4 KB anywhere in 64-bit address range	Thermal Reporting	Enable using standard PCI mechanism (D31:F6 TBARB/ TBARBH)
16 Bytes anywhere in 64-bit address range	Intel® MEI #1, #2	Enable using standard PCI mechanism (D22:F 1:0)
4 KB anywhere in 4 GB range	KT	Enable using standard PCI mechanism (D22:F3)
16 KB anywhere in 4 GB range	Root Complex Register Block (RCRB)	Enable using setting bit[0] of the Root Complex Base Address register (D31:F0:offset F0h).

Notes:
1. Software must not attempt locks to memory mapped I/O ranges for USB EHCI or High Precision Event Timers. If attempted, the lock is not honored, which means potential deadlock conditions may occur.
2. PCI is the target when the Boot BIOS Destination selection bits are set to 10b (Chipset Config Registers:Offset 3401 bits 11:10). When PCI selected, the Firmware Hub Decode Enable bits have no effect.

4.4.1 Boot-Block Update Scheme

Intel® Xeon® Processor D-1500 Product Family supports a "Top Swap" mode that has Intel® Xeon® Processor D-1500 Product Family swap the top block in the FWH or SPI flash (the boot-block) with another location. This allows for safe update of the boot-block (even if a power failure occurs). When the "Top Swap" Enable bit is set, Intel® Xeon® Processor D-1500 Product Family will invert A16 for cycles going to the upper two 64 KB blocks in the FWH or appropriate address lines as selected in BIOS Boot-Block size soft strap for SPI.

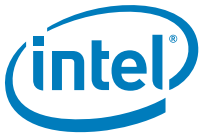
Specifically for FHW, in this mode accesses to FFFF_0000h–FFFF_FFFFh are directed to FFFE_0000h–FFFE_FFFFh and vice versa. When the Top Swap Enable bit is 0, Intel® Xeon® Processor D-1500 Product Family will not invert A16.

Specifically for SPI, in this mode the "Top Swap" behavior is as described below. When the Top Swap Enable bit is 0, Intel® Xeon® Processor D-1500 Product Family will not invert any address bit.

Table 4-5. SPI Mode Address Swapping

BIOS Boot-Block size Value	Accesses to	Being Directed to
000 (64 KB)	FFFF_0000h–FFFF_FFFFh	FFFE_0000h–FFFE_FFFFh and vice versa
001 (128 KB)	FFFE_0000h–FFFF_FFFFh	FFFC_0000h–FFFD_FFFFh and vice versa
010 (256 KB)	FFFC_0000h–FFFF_FFFFh	FFF8_0000h–FFFB_FFFFh and vice versa
011 (512 KB)	FFF8_0000h–FFFF_FFFFh	FFF0_0000h–FFF7_FFFFh and vice versa
100 (1 MB)	FFF0_0000h–FFFF_FFFFh	FFE0_0000h–FFEF_FFFFh and vice versa
101–111	Reserved	Reserved

This bit is automatically set to 0 by RTCRST#, but not by PLTRST#.



The scheme is based on the concept that the top block is reserved as the “boot” block, and the block immediately below the top block is reserved for doing boot-block updates.

The algorithm is:

1. Software copies the top block to the block immediately below the top
2. Software checks that the copied block is correct. This could be done by performing a checksum calculation.
3. Software sets the Top Swap bit. This will invert the appropriate address bits for the cycles going to the FWH or SPI.
4. Software erases the top block
5. Software writes the new top block
6. Software checks the new top block
7. Software clears the Top Swap bit

If a power failure occurs at any point after step 3, the system will be able to boot from the copy of the boot-block that is stored in the block below the top. This is because the Top Swap bit is backed in the RTC well.

Note: The “Top Swap” mode may be forced by an external strapping option. When top swap mode is forced in this manner, the Top Swap bit cannot be cleared by software. A re-boot with the strap removed will be required to exit a forced top-block swap mode.

Note: Top swap mode only affects accesses to the Firmware Hub space, not feature space for FWH.

Note: The top swap mode has no effect on accesses below FFFE_0000h for FWH.

§

5 Chipset Configuration Registers

This section describes all registers and base functionality that is related to chipset configuration and not a specific interface (such as LPC, USB, or PCI Express*). It contains the root complex register block that describes the behavior of the upstream internal link.

This block is mapped into memory space, using the Root Complex Base Address (RCBA) register of the PCI-to-LPC bridge. Accesses in this space must be limited to 32 bit (DW) quantities. Burst accesses are not allowed.

5.1 Chipset Configuration Registers (Memory Space)

Note: Address locations that are not shown should be treated as Reserved (see Section 4.2 for details).

Table 5-1. Chipset Configuration Register Memory Map (Memory Space) (Sheet 1 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
0400h–0403	RPC	Root Port Configuration	0000000yh	R/W, RO
0404h–0407h	RPFN	Root Port Function Number and Hide for PCI Express Root Ports	76543210h	R/W, R/WO
0408h–040Bh	FLRSTAT	Function Level Reset Pending Status Summary	00000000h	RO/V
1E00h–1E03h	TRSR	Trap Status	00000000h	R/WC, RO
1E10h–1E17h	TRCR	Trapped Cycle	0000000000000000h	RO
1E18h–1E1Fh	TWDR	Trapped Write Data	0000000000000000h	RO
1E80h–1E87h	IOTR0	I/O Trap Register 0	0000000000000000h	R/W
1E88h–1E8Fh	IOTR1	I/O Trap Register 1	0000000000000000h	R/W
1E90h–1E97h	IOTR2	I/O Trap Register 2	0000000000000000h	R/W
1E98h–1E9Fh	IOTR3	I/O Trap Register 3	0000000000000000h	R/W
2014h–2017h	V0CTL	Virtual Channel 0 Resource Control	80000010h	R/WL, RO
201Ah–201Bh	V0STS	Virtual Channel 0 Resource Status	0000h	RO
2020h–2023h	V1CTL	Virtual Channel 1 Resource Control	00000000h	R/W, RO, R/WL
2026h–2027h	V1STS	Virtual Channel 1 Resource Status	0000h	RO
20ACh–20AFh	REC	Root Error Command	0000h	R/W
3000h	TCTL	TCO Configuration	00h	R/W
3100h–3103h	D31IP	Device 31 Interrupt Pin	03243200h	R/W, RO
3104h–3107h	D30IP	Device 30 Interrupt Pin	00000000h	RO
3108h–310Bh	D29IP	Device 29 Interrupt Pin	10004321h	R/W
310Ch–310Fh	D28IP	Device 28 Interrupt Pin	00214321h	R/W
3110h–3113h	D27IP	Device 27 Interrupt Pin	00000001h	R/W
3114h–3117h	D26IP	Device 26 Interrupt Pin	30000321h	R/W
3118h–311Bh	D25IP	Device 25 Interrupt Pin	00000001h	R/W
3124h–3127h	D22IP	Device 22 Interrupt Pin	00004321h	R/W
3128h–312Bh	D20IP	Device 20 Interrupt Pin	00000021h	R/W

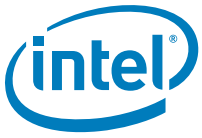


Table 5-1. Chipset Configuration Register Memory Map (Memory Space) (Sheet 2 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
3140h–3141h	D31IR	Device 31 Interrupt Route	3210h	R/W
3144h–3145h	D29IR	Device 29 Interrupt Route	3210h	R/W
3146h–3147h	D28IR	Device 28 Interrupt Route	3210h	R/W
3148h–3149h	D27IR	Device 27 Interrupt Route	3210h	R/W
314Ch–314Dh	D26IR	Device 26 Interrupt Route	3210h	R/W
3150h–3151h	D25IR	Device 25 Interrupt Route	3210h	R/W
315Ch–315Dh	D22IR	Device 22 Interrupt Route	3210h	R/W
3160h–3161h	D20IR	Device 20 Interrupt Route	3210h	R/W
31FEh–31FFh	OIC	Other Interrupt Control	0000h	R/W
3300h–3303h	WADT_AC	Wake Alarm Device Timer – AC	FFFFFFFFh	R/W
3304h–3307h	WADT_DC	Wake Alarm Device Timer – DC	FFFFFFFFh	R/W
3308h–330Bh	WADT_EXP_AC	Wake Alarm Device Expired Timer – AC	FFFFFFFFh	R/W
330Ch–330Fh	WADT_EXP_DC	Wake Alarm Device Expired Timer – DC	FFFFFFFFh	R/W
3310h–3313h	PRSTS	Power and Reset Status	05000000h	RO, R/WC
3318h–331Bh	PM_CFG	Power Management Configuration	00000020h	R/W
33C8h–33CBh	PMSYNC_CFG	PMSYNC Configuration	00000000h	R/W
3400h–3403h	RC	RTC Configuration	00000000h	R/W, R/WLO
3404h–3407h	HPTC	High Precision Timer Configuration	00000000h	R/W
3410h–3413h	GCS	General Control and Status	000000yy0h	R/W, R/WLO
3414h	BUC	Backed Up Control	00h	R/W
3418h–341Bh	FD	Function Disable	00000000h	R/W
341Ch–341Fh	CG	Clock Gating	00000000h	R/W
3424h–3425h	DISPBDF	Display Bus, Device and Function Initialization	00040010h	R/W
3428h–342Bh	FD2	Function Disable 2	00000000h	R/W

5.1.1 RPC—Root Port Configuration Register

Offset Address: 0400–0403h Attribute: R/W, RO
Default Value: 0000000yh (y = 00xxb) Size: 32-bit

Bit	Description
31:0	Reserved. BIOS may write to this register, as needed.

5.1.2 RPFN—Root Port Function Number and Hide for PCI Express* Root Ports Register

Offset Address: 0404–0407h Attribute: R/W, R/WO
Default Value: 76543210h Size: 32-bit

For the PCI Express root ports, the assignment of a function number to a root port is not fixed. BIOS may re-assign the function numbers on a port by port basis. This capability will allow BIOS to disable/hide any root port and still have functions 0 thru N-1 where N is the total number of enabled root ports.

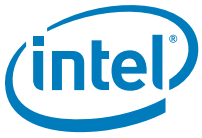
Port numbers will remain fixed to a physical root port.

The existing root port Function Disable registers operate on physical ports (not functions).

Port Configuration (1x4, 4x1, and so on) is not affected by the logical function number assignment and is associated with physical ports.

Note: The difference between hiding vs disabling a port is that a hidden port is not able to claim downstream Config cycles **only**. Memory and I/O cycles are still claimed by that hidden port. A disabled port is turned off and not able to claim downstream Configuration, Memory and I/O cycles – it saves power.Function disable is covered in Chapter 5, "FD—Function Disable Register".

Bit	Description
31	**Root Port 8 Config Hide (RP8CH)** — R/W. This bit is used to hide the root port and any devices behind it from being discovered by the OS. When set to 1, the root port will not claim any downstream configuration transactions.
30:28	**Root Port 8 Function Number (RP8FN)** — R/WO. These bits set the function number for PCI Express* Root Port 8. This root port function number must be a unique value from the other root port function numbers
27	**Root Port 7 Config Hide (RP7CH)** — R/W. This bit is used to hide the root port and any devices behind it from being discovered by the OS. When set to 1, the root port will not claim any downstream configuration transactions.
26:24	**Root Port 7 Function Number (RP7FN)** — R/WO. These bits set the function number for PCI Express Root Port 7. This root port function number must be a unique value from the other root port function numbers
23	**Root Port 6 Config Hide (RP6CH)** — R/W. This bit is used to hide the root port and any devices behind it from being discovered by the OS. When set to 1, the root port will not claim any downstream configuration transactions.
22:20	**Root Port 6 Function Number (RP6FN)** — R/WO. These bits set the function number for PCI Express Root Port 6. This root port function number must be a unique value from the other root port function numbers
19	**Root Port 5 Config Hide (RP5CH)** — R/W. This bit is used to hide the root port and any devices behind it from being discovered by the OS. When set to 1, the root port will not claim any downstream configuration transactions.
18:16	**Root Port 5 Function Number (RP5FN)** — R/WO. These bits set the function number for PCI Express Root Port 5. This root port function number must be a unique value from the other root port function numbers
15	**Root Port 4 Config Hide (RP4CH)** — R/W. This bit is used to hide the root port and any devices behind it from being discovered by the OS. When set to 1, the root port will not claim any downstream configuration transactions.
14:12	**Root Port 4 Function Number (RP4FN)** — R/WO. These bits set the function number for PCI Express Root Port 4. This root port function number must be a unique value from the other root port function numbers
11	**Root Port 3 Config Hide (RP3CH)** — R/W. This bit is used to hide the root port and any devices behind it from being discovered by the OS. When set to 1, the root port will not claim any downstream configuration transactions.
10:8	**Root Port 3 Function Number (RP3FN)** — R/WO. These bits set the function number for PCI Express Root Port 3. This root port function number must be a unique value from the other root port function numbers
7	**Root Port 2 Config Hide (RP2CH)** — R/W. This bit is used to hide the root port and any devices behind it from being discovered by the OS. When set to 1, the root port will not claim any downstream configuration transactions.
6:4	**Root Port 2 Function Number (RP2FN)** — R/WO. These bits set the function number for PCI Express* Root Port 2. This root port function number must be a unique value from the other root port function numbers
3	**Root Port 1 Config Hide (RP1CH)** — R/W. This bit is used to hide the root port and any devices behind it from being discovered by the OS. When set to 1, the root port will not claim any downstream configuration transactions.
2:0	**Root Port 1 Function Number (RP1FN)** — R/WO. These bits set the function number for PCI Express Root Port 1. This root port function number must be a unique value from the other root port function numbers



5.1.3 FLRSTAT—Function Level Reset Pending Status Register

Offset Address: 0408–040Bh Attribute: RO/V
Default Value: 00000000h Size: 32-bit

Bit	Description
31:24	Reserved
23	FLR Pending Status for D29:F0, EHCI #1 — RO/V. 0 = Function Level Reset is not pending. 1 = Function Level Reset is pending.
22:16	Reserved
15	FLR Pending Status for D26:F0, EHCI #2 — RO/V. 0 = Function Level Reset is not pending. 1 = Function Level Reset is pending.
14:0	Reserved

5.1.4 TRSR—Trap Status Register

Offset Address: 1E00–1E03h Attribute: R/WC, RO
Default Value: 00000000h Size: 32-bit

Bit	Description
31:4	Reserved
3:0	**Cycle Trap SMI# Status (CTSS)** — R/WC. These bits are set by hardware when the corresponding Cycle Trap register is enabled and a matching cycle is received (and trapped). These bits are OR'ed together to create a single status bit in the Power Management register space. The SMI# and trapping must be enabled in order to set these bits. These bits are set before the completion is generated for the trapped cycle, thereby ensuring that the processor can enter the SMI# handler when the instruction completes. Each status bit is cleared by writing a 1 to the corresponding bit location in this register.

5.1.5 TRCR—Trapped Cycle Register

Offset Address: 1E10–1E17h Attribute: RO
Default Value: 0000000000000000h Size: 64-bit

This register saves information about the I/O Cycle that was trapped and generated the SMI# for software to read.

Bit	Description
63:25	Reserved
24	**Read/Write# (RWI)** — RO. 0 = Trapped cycle was a write cycle. 1 = Trapped cycle was a read cycle.
23:20	Reserved
19:16	**Active-high Byte Enables (AHBE)** — RO. This is the DWord-aligned byte enables associated with the trapped cycle. A 1 in any bit location indicates that the corresponding byte is enabled in the cycle.
15:2	**Trapped I/O Address (TIOA)** — RO. This is the DWord-aligned address of the trapped cycle.
1:0	Reserved

5.1.6 TWDR—Trapped Write Data Register

Offset Address:	1E18–1E1Fh	Attribute:	RO
Default Value:	0000000000000000h	Size:	64-bit

This register saves the data from I/O write cycles that are trapped for software to read.

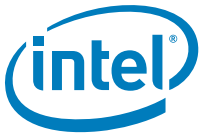
Bit	Description
63:32	Reserved
31:0	**Trapped I/O Data (TIOD)** — RO. DWord of I/O write data. This field is undefined after trapping a read cycle.

5.1.7 IOTRn—I/O Trap Register (0–3)

Offset Address:	1E80–1E87h Register 0 1E88–1E8Fh Register 1 1E90–1E97h Register 2 1E98–1E9Fh Register 3	Attribute:	R/W
Default Value:	0000000000000000h	Size:	64-bit

These registers are used to specify the set of I/O cycles to be trapped and to enable this functionality.

Bit	Description
63:50	Reserved
49	**Read/Write Mask (RWM)** — R/W. 0 = The cycle must match the type specified in bit 48. 1 = Trapping logic will operate on both read and write cycles.
48	**Read/Write# (RWIO)** — R/W. 0 = Write 1 = Read ***Note:*** The value in this field does not matter if bit 49 is set.
47:40	Reserved
39:36	**Byte Enable Mask (BEM)** — R/W. A 1 in any bit position indicates that any value in the corresponding byte enable bit in a received cycle will be treated as a match. The corresponding bit in the Byte Enables field, below, is ignored.
35:32	**Byte Enables (TBE)** — R/W. Active-high DWord-aligned byte enables.
31:24	Reserved
23:18	**Address[7:2] Mask (ADMA)** — R/W. A 1 in any bit position indicates that any value in the corresponding address bit in a received cycle will be treated as a match. The corresponding bit in the Address field, below, is ignored. The mask is only provided for the lower 6 bits of the DWord address, allowing for traps on address ranges up to 256 bytes in size.
17:16	Reserved
15:2	**I/O Address[15:2] (IOAD)** — R/W. DWord-aligned address
1	Reserved
0	**Trap and SMI# Enable (TRSE)** — R/W. 0 = Trapping and SMI# logic disabled. 1 = The trapping logic specified in this register is enabled.



5.1.8 V0CTL—Virtual Channel 0 Resource Control Register

Offset Address: 2014–2017h
Attribute: R/WL, RO
Default Value: 80000010h
Size: 32-bit

Bit	Description
31	**Virtual Channel Enable (EN)** — RO. Always set to 1. VC0 is always enabled and cannot be disabled.
30:27	Reserved
26:24	**Virtual Channel Identifier (ID)** — RO. Indicates the ID to use for this virtual channel.
23:16	Reserved
15:10	**Extended TC/VC Map (ETVM)**— R/WL. Defines the upper 8-bits of the VC0 16-bit TC/VC mapping registers. These registers use the PCI Express reserved TC[3] traffic class bit. These bits are locked if the TCLOCKDN bit (RCBA+0050h:bit 31) is set.
9:7	Reserved
6:1	**Transaction Class / Virtual Channel Map (TVM)** — R/WL. Indicates which transaction classes are mapped to this virtual channel. When a bit is set, this transaction class is mapped to the virtual channel. These bits are locked if the TCLOCKDN bit (RCBA+0050h:bit 31) is set.
0	Reserved

5.1.9 V0STS—Virtual Channel 0 Resource Status Register

Offset Address: 201A–201Bh
Attribute: RO
Default Value: 0000h
Size: 16-bit

Bit	Description
15:2	Reserved
1	**VC Negotiation Pending (NP)** — RO. When set, this bit indicates the virtual channel is still being negotiated with ingress ports.
0	Reserved

5.1.10 V1CTL—Virtual Channel 1 Resource Control Register

Offset Address: 2020–2023h
Attribute: R/W, RO, R/WL
Default Value: 00000000h
Size: 32-bit

Bit	Description
31	**Virtual Channel Enable (EN)** — R/W. Enables the VC when set. Disables the VC when cleared.
30:28	Reserved
27:24	**Virtual Channel Identifier (ID)** — R/W. Indicates the ID to use for this virtual channel.
23:16	Reserved
15:10	**Extended TC/VC Map (ETVM)** — R/WL. Defines the upper 8-bits of the VC0 16-bit TC/VC mapping registers. These registers use the PCI Express* reserved TC[3] traffic class bit. These bits are locked if the TCLOCKDN bit (RCBA+0050h:bit 31) is set.
9:8	Reserved
7:1	**Transaction Class / Virtual Channel Map (TVM)** — R/WL. Indicates which transaction classes are mapped to this virtual channel. When a bit is set, this transaction class is mapped to the virtual channel. These bits are locked if the TCLOCKDN bit (RCBA+0050h:bit 31) is set.
0	Reserved

5.1.11 V1STS—Virtual Channel 1 Resource Status Register

Offset Address: 2026–2027h Attribute: RO
Default Value: 0000h Size: 16-bit

Bit	Description
15:2	Reserved
1	**VC Negotiation Pending (NP)** — RO. When set, this bit indicates the virtual channel is still being negotiated with ingress ports.
0	Reserved

5.1.12 REC—Root Error Command Register

Offset Address: 20AC–20AFh Attribute: R/W
Default Value: 0000h Size: 32-bit

Bit	Description
31	**Drop Poisoned Downstream Packets (DPDP)** — R/W. Determines how downstream packets for internal messaging are handled that are received with the EP field set, indicating poisoned data: 0 = Packets are forwarded downstream without forcing the UT field set. 1 = This packet and all subsequent packets with data received internally for any VC will have their Unsupported Transaction (UT) field set causing them to master Abort downstream. Packets without data such as memory, I/O and config read requests are allowed to proceed.
30:0	Reserved

5.1.13 CIR2314—Chipset Initialization Register 2314

Offset Address: 2314–2317h Attribute: R/W
Default Value: 0A000000h Size: 32-bit

Bit	Description
31:0	**CIR2314 Field 1** — R/W. BIOS may program this field.

5.1.14 CIR2320—Chipset Initialization Register 2320

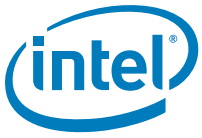
Offset Address: 2320–2323h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR2320 Field 1** — R/W. BIOS may program this field.

5.1.15 TCTL—TCO Configuration Register

Offset Address: 3000h Attribute: R/W
Default Value: 00h Size: 8-bit

Bit	Description
7	**TCO IRQ Enable (IE)** — R/W. 0 = TCO IRQ is disabled. 1 = TCO IRQ is enabled, as selected by the TCO_IRQ_SEL field.
6:3	Reserved



Bit	Description
2:0	**TCO IRQ Select (IS)** — R/W. Specifies on which IRQ the TCO will internally appear. If not using the APIC, the TCO interrupt must be routed to IRQ9–11, and that interrupt is not sharable with the SERIRQ stream, but is shareable with other PCI interrupts. If using the APIC, the TCO interrupt can also be mapped to IRQ20–23, and can be shared with other interrupt. 000 = IRQ 9 001 = IRQ 10 010 = IRQ 11 011 = Reserved 100 = IRQ 20 (only if APIC enabled) 101 = IRQ 21 (only if APIC enabled) 110 = IRQ 22 (only if APIC enabled) 111 = IRQ 23 (only if APIC enabled) When setting the these bits, the IE bit should be cleared to prevent glitching. When the interrupt is mapped to APIC interrupts 9, 10, or 11, the APIC should be programmed for active-high reception. When the interrupt is mapped to APIC interrupts 20 through 23, the APIC should be programmed for active-low reception.

5.1.16 D31IP—Device 31 Interrupt Pin Register

Offset Address: 3100–3103h Attribute: R/W, RO
Default Value: 03243200h Size: 32-bit

Bit	Description
31:28	Reserved
27:24	**Thermal Throttle Pin (TTIP)** — R/W. Indicates which pin the Thermal Throttle controller drives as its interrupt. 0h = No interrupt 1h = INTA# 2h = INTB# 3h = INTC# (**Default**) 4h = INTD# 5h–Fh = Reserved
23:20	**SATA Pin 2 (SIP2)** — R/W. Indicates which pin the SATA controller 2 drives as its interrupt. 0h = No interrupt 1h = INTA# 2h = INTB# (**Default**) 3h = INTC# 4h = INTD# 5h–Fh = Reserved
19:16	Reserved
15:12	**SMBus Pin (SMIP)** — R/W. Indicates which pin the SMBus controller drives as its interrupt. 0h = No interrupt 1h = INTA# 2h = INTB# 3h = INTC# (**Default**) 4h = INTD# 5h–Fh = Reserved
11:8	**SATA Pin (SIP)** — R/W. Indicates which pin the SATA controller drives as its interrupt. 0h = No interrupt 1h = INTA# 2h = INTB# (**Default**) 3h = INTC# 4h = INTD# 5h–Fh = Reserved
7:4	Reserved
3:0	**LPC Bridge Pin (LIP)** — RO. Currently, the LPC bridge does not generate an interrupt, so this field is read-only and 0h.

5.1.17 D30IP—Device 30 Interrupt Pin Register

Offset Address: 3104–3107h Attribute: RO
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	Reserved

5.1.18 D29IP—Device 29 Interrupt Pin Register

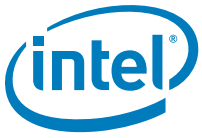
Offset Address: 3108–310Bh Attribute: R/W
Default Value: 10004321h Size: 32-bit

Bit	Description
31:4	Reserved
3:0	**EHCI #1 Pin (E1P)** — R/W. Indicates which pin the EHCI controller #1 drives as its interrupt, if controller exists. 0h = No interrupt 1h = INTA# (Default) 2h = INTB# 3h = INTC# 4h = INTD# 5h–7h = Reserved ***Note:*** EHCI Controller #1 is mapped to Device 29 Function 0.

5.1.19 D28IP—Device 28 Interrupt Pin Register

Offset Address: 310C–310Fh Attribute: R/W
Default Value: 00214321h Size: 32-bit

Bit	Description
31:28	**PCI Express* #8 Pin (P8IP)** — R/W. Indicates which pin the PCI Express* port #8 drives as its interrupt. 0h = No interrupt 1h = INTA# 2h = INTB# 3h = INTC# 4h = INTD# (**Default**) 5h–7h = Reserved
27:24	**PCI Express #7 Pin (P7IP)** — R/W. Indicates which pin the PCI Express port #7 drives as its interrupt. 0h = No interrupt 1h = INTA# 2h = INTB# 3h = INTC# (**Default**) 4h = INTD# 5h–7h = Reserved
23:20	**PCI Express* #6 Pin (P6IP)** — R/W. Indicates which pin the PCI Express* port #6 drives as its interrupt. 0h = No interrupt 1h = INTA# 2h = INTB# (**Default**) 3h = INTC# 4h = INTD# 5h–7h = Reserved
19:16	**PCI Express #5 Pin (P5IP)** — R/W. Indicates which pin the PCI Express port #5 drives as its interrupt. 0h = No interrupt 1h = INTA# (**Default**) 2h = INTB# 3h = INTC# 4h = INTD# 5h–7h = Reserved



Bit	Description
15:12	**PCI Express #4 Pin (P4IP)** — R/W. Indicates which pin the PCI Express* port #4 drives as its interrupt. 0h = No interrupt 1h = INTA# 2h = INTB# 3h = INTC# 4h = INTD# (**Default**) 5h–7h = Reserved
11:8	**PCI Express #3 Pin (P3IP)** — R/W. Indicates which pin the PCI Express port #3 drives as its interrupt. 0h = No interrupt 1h = INTA# 2h = INTB# 3h = INTC# (**Default**) 4h = INTD# 5h–7h = Reserved
7:4	**PCI Express #2 Pin (P2IP)** — R/W. Indicates which pin the PCI Express port #2 drives as its interrupt. 0h = No interrupt 1h = INTA# 2h = INTB# (**Default**) 3h = INTC# 4h = INTD# 5h–7h = Reserved
3:0	**PCI Express #1 Pin (P1IP)** — R/W. Indicates which pin the PCI Express port #1 drives as its interrupt. 0h = No interrupt 1h = INTA# (**Default**) 2h = INTB# 3h = INTC# 4h = INTD# 5h–7h = Reserved

5.1.20 D27IP—Device 27 Interrupt Pin Register

Offset Address: 3110–3113h Attribute: R/W
Default Value: 00000001h Size: 32-bit

Bit	Description
31:0	Reserved

5.1.21 D26IP—Device 26 Interrupt Pin Register

Offset Address: 3114–3117h Attribute: R/W
Default Value: 30000321h Size: 32-bit

Bit	Description
31:4	Reserved
3:0	**EHCI #2 Pin (E2P)** — R/W. Indicates which pin EHCI controller #2 drives as its interrupt, if controller exists. 0h = No Interrupt 1h = INTA# (Default) 2h = INTB# 3h = INTC# 4h = INTD# 5h–Fh = Reserve ***Note:*** EHCI Controller #2 is mapped to Device 26 Function 0.

5.1.22 D25IP—Device 25 Interrupt Pin Register

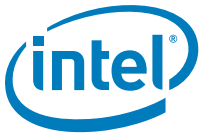
Offset Address: 3118–311Bh Attribute: R/W
Default Value: 00000001h Size: 32-bit

Bit	Description
31:4	Reserved
3:0	**GbE LAN Pin (LIP)** — R/W. Indicates which pin the internal GbE LAN controller drives as its interrupt 0h = No Interrupt 1h = INTA# (**Default**) 2h = INTB# 3h = INTC# 4h = INTD# 5h–Fh = Reserved

5.1.23 D22IP—Device 22 Interrupt Pin Register

Offset Address: 3124–3127h Attribute: R/W
Default Value: 00004321h Size: 32-bit

Bit	Description
31:16	Reserved
15:12	**KT Pin (KTIP)** — R/W. Indicates which pin the Keyboard text PCI functionality drives as its interrupt 0h = No Interrupt 1h = INTA# 2h = INTB# 3h = INTC# 4h = INTD# (**Default**) 5h–Fh = Reserved
11:8	**IDE-R Pin (IDERIP)** — R/W. Indicates which pin the IDE Redirect PCI functionality drives as its interrupt 0h = No Interrupt 1h = INTA# 2h = INTB# 3h = INTC# (**Default**) 4h = INTD# 5h–Fh = Reserved
7:4	**Intel® MEI #2 Pin (MEI2IP)** — R/W. Indicates which pin the Management Engine Interface #2 drives as its interrupt 0h = No Interrupt 1h = INTA# 2h = INTB# (**Default**) 3h = INTC# 4h = INTD# 5h–Fh = Reserved
3:0	**Intel® MEI #1 Pin (MEI1IP)** — R/W. Indicates which pin the Management Engine Interface controller #1 drives as its interrupt 0h = No Interrupt 1h = INTA# (**Default**) 2h = INTB# 3h = INTC# 4h = INTD# 5h–Fh = Reserved



5.1.24 D20IP—Device 20 Interrupt Pin Register

Offset Address: 3128–312bh
Attribute: R/W
Default Value: 00000021h
Size: 32-bit

Bit	Description
31:4	Reserved
3:0	**xHCI Pin (XHCIIP)** — R/W. Indicates which pin the xHCI drives as its interrupt 0h = No Interrupt 1h = INTA# (**Default**) 2h = INTB# 3h = INTC# 4h = INTD# 5h–Fh = Reserved

5.1.25 D31IR—Device 31 Interrupt Route Register

Offset Address: 3140–3141h
Attribute: R/W
Default Value: 3210h
Size: 16-bit

Bit	Description
15	Reserved
14:12	**Interrupt D Pin Route (IDR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTD# pin reported for device 31 functions. 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# (Default) 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
11	Reserved
10:8	**Interrupt C Pin Route (ICR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTC# pin reported for device 31 functions. 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# (Default) 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
7	Reserved
6:4	**Interrupt B Pin Route (IBR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTB# pin reported for device 31 functions. 0h = PIRQA# 1h = PIRQB# (Default) 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
3	Reserved
2:0	**Interrupt A Pin Route (IAR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTA# pin reported for device 31 functions. 0h = PIRQA# (Default) 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#

5.1.26 D30IR—Device 30 Interrupt Route Register

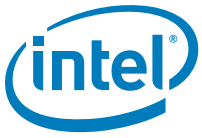
Offset Address: 3142–3143h Attribute: RO
Default Value: 0000h Size: 16-bit

Bit	Description
15:0	Reserved. No interrupts generated from Device 30.

5.1.27 D29IR—Device 29 Interrupt Route Register

Offset Address: 3144–3145h Attribute: R/W
Default Value: 3210h Size: 16-bit

Bit	Description
15	Reserved
14:12	**Interrupt D Pin Route (IDR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTD# pin reported for device 29 functions. 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# (Default) 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
11	Reserved
10:8	**Interrupt C Pin Route (ICR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTC# pin reported for device 29 functions. 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# (Default) 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
7	Reserved
6:4	**Interrupt B Pin Route (IBR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTB# pin reported for device 29 functions. 0h = PIRQA# 1h = PIRQB# (Default) 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
3	Reserved
2:0	**Interrupt A Pin Route (IAR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTA# pin reported for device 29 functions. 0h = PIRQA# (Default) 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#



5.1.28 D28IR—Device 28 Interrupt Route Register

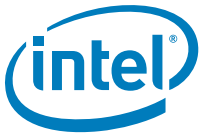
Offset Address: 3146–3147h
Default Value: 3210h
Attribute: R/W
Size: 16-bit

Bit	Description
15	Reserved
14:12	**Interrupt D Pin Route (IDR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTD# pin reported for device 28 functions. 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# (Default) 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
11	Reserved
10:8	**Interrupt C Pin Route (ICR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTC# pin reported for device 28 functions. 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# (Default) 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
7	Reserved
6:4	**Interrupt B Pin Route (IBR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTB# pin reported for device 28 functions. 0h = PIRQA# 1h = PIRQB# (Default) 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
3	Reserved
2:0	**Interrupt A Pin Route (IAR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTA# pin reported for device 28 functions. 0h = PIRQA# (Default) 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#

5.1.29 D27IR—Device 27 Interrupt Route Register

Offset Address: 3148–3149h
Attribute: R/W
Default Value: 3210h
Size: 16-bit

Bit	Description
15	Reserved
14:12	**Interrupt D Pin Route (IDR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTD# pin reported for device 27 functions. 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# (Default) 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
11	Reserved
10:8	**Interrupt C Pin Route (ICR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTC# pin reported for device 27 functions. 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# (Default) 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
7	Reserved
6:4	**Interrupt B Pin Route (IBR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTB# pin reported for device 27 functions. 0h = PIRQA# 1h = PIRQB# (Default) 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
3	Reserved
2:0	**Interrupt A Pin Route (IAR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTA# pin reported for device 27 functions. 0h = PIRQA# (Default) 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#



5.1.30 D26IR—Device 26 Interrupt Route Register

Offset Address: 314C–314Dh Attribute: R/W
Default Value: 3210h Size: 16-bit

Bit	Description
15	Reserved
14:12	**Interrupt D Pin Route (IDR) —** R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTD# pin reported for device 26 functions: 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# (Default) 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
11	Reserved
10:8	**Interrupt C Pin Route (ICR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTC# pin reported for device 26 functions. 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# (Default) 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
7	Reserved
6:4	**Interrupt B Pin Route (IBR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTB# pin reported for device 26 functions. 0h = PIRQA# 1h = PIRQB# (Default) 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
3	Reserved
2:0	**Interrupt A Pin Route (IAR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTA# pin reported for device 26 functions. 0h = PIRQA# (Default) 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#

5.1.31 D25IR—Device 25 Interrupt Route Register

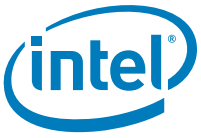
Offset Address: 3150–3151h
Attribute: R/W
Default Value: 3210h
Size: 16-bit

Bit	Description
15	Reserved
14:12	**Interrupt D Pin Route (IDR):** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTD# pin reported for device 25 functions: 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# (Default) 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
11	Reserved
10:8	**Interrupt C Pin Route (ICR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTC# pin reported for device 25 functions. 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# (Default) 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
7	Reserved
6:4	**Interrupt B Pin Route (IBR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTB# pin reported for device 25 functions. 0h = PIRQA# 1h = PIRQB# (Default) 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
3	Reserved
2:0	**Interrupt A Pin Route (IAR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTA# pin reported for device 25 functions. 0h = PIRQA# (Default) 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#

5.1.32 D22IR—Device 22 Interrupt Route Register

Offset Address: 315C–315Dh Attribute: R/W
Default Value: 3210h Size: 16-bit

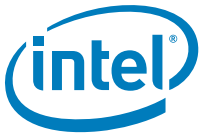
Bit	Description
15	Reserved
14:12	**Interrupt D Pin Route (IDR):** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTD# pin reported for device 22 functions: 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# (Default) 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
11	Reserved
10:8	**Interrupt C Pin Route (ICR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTC# pin reported for device 22 functions. 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# (Default) 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
7	Reserved
6:4	**Interrupt B Pin Route (IBR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTB# pin reported for device 22 functions. 0h = PIRQA# 1h = PIRQB# (Default) 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
3	Reserved
2:0	**Interrupt A Pin Route (IAR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTA# pin reported for device 22 functions. 0h = PIRQA# (Default) 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#



5.1.33 D20IR—Device 20 Interrupt Route Register

Offset Address: 3160–3161h
Attribute: R/W
Default Value: 3210h
Size: 16-bit

Bit	Description
15	Reserved
14:12	**Interrupt D Pin Route (IDR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTD# pin reported for device 20 functions: 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# (Default) 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
11	Reserved
10:8	**Interrupt C Pin Route (ICR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTC# pin reported for device 20 functions. 0h = PIRQA# 1h = PIRQB# 2h = PIRQC# (Default) 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
7	Reserved
6:4	**Interrupt B Pin Route (IBR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTB# pin reported for device 20 functions. 0h = PIRQA# 1h = PIRQB# (Default) 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#
3	Reserved
2:0	**Interrupt A Pin Route (IAR)** — R/W. Indicates which physical pin on Intel® Xeon® Processor D-1500 Product Family is connected to the INTA# pin reported for device 20 functions. 0h = PIRQA# (Default) 1h = PIRQB# 2h = PIRQC# 3h = PIRQD# 4h = PIRQE# 5h = PIRQF# 6h = PIRQG# 7h = PIRQH#



5.1.34 OIC—Other Interrupt Control Register

Offset Address: 31FE–31FFh Attribute: R/W
Default Value: 0000h Size: 16-bit

Bit	Description
15:10	Reserved
9	**Coprocessor Error Enable (CEN)** — R/W. 0 = FERR# will not generate IRQ13 nor IGNNE#. 1 = If FERR# is low, Intel® Xeon® Processor D-1500 Product Family generates IRQ13 internally and holds it until an I/O port F0h write. It will also drive IGNNE# active.
8	**APIC Enable (AEN)** — R/W. 0 = The internal IOxAPIC is disabled. 1 = Enables the internal IOxAPIC and its address decode. ***Note:*** Software should read this register after modifying APIC enable bit prior to access to the IOxAPIC address range.
7:0	**APIC Range Select (ASEL)** — R/W. These bits define address bits 19:12 for the IOxAPIC range. The default value of 00h enables compatibility with prior Intel® Xeon® Processor D-1500 Product Family products as an initial value. This value must not be changed unless the IOxAPIC Enable bit is cleared.

Note: FEC1_0000h–FEC3_FFFFh is allocated to PCIe when I/OxAPIC Enable (PAE) bit is set.

5.1.35 WADT_AC—Wake Alarm Device Timer – AC Register

Offset Address: 3300–3303h Attribute: R/W
Default Value: FFFFFFFFh Size: 32-bit

Bit	Description
31:0	**Wake Alarm Device Timer Value for AC Mode (WADT_AC_VAL):** R/W. This field contains the 32-bit wake alarm device timer value (1 second granularity) for AC power. The timer begins decrementing when written to a value other than FFFFFFFFh (regardless of the power source when the write occurs). Upon counting down to 0: • If on AC power, GPE0_STS.WADT_STS will be set. This status bit being set will generate a host wake if GPE0_EN.WADT_EN is '1'. • If power source is DC at this time, the status bit is not set. However, if AC power subsequently returns to the platform, the AC Expired Timer begins running. Refer to WADT_EXP_AC for more details. • The timer returns to its default value of FFFFFFFFh.

5.1.36 WADT_DC—Wake Alarm Device Timer – DC Register

Offset Address: 3304–3307h Attribute: R/W
Default Value: FFFFFFFFh Size: 32-bit

Bit	Description
31:0	**Wake Alarm Device Timer Value for DC Mode (WADT_DC_VAL):** R/W. This field contains the 32-bit wake alarm device timer value (1 second granularity) for DC power. The timer begins decrementing when written to a value other than FFFFFFFFh (regardless of the power source when the write occurs). Upon counting down to 0: • If on DC power, GPE0_STS.WADT_STS will be set. This status bit being set will generate a host wake if GPE0_EN.WADT_EN is '1'. • If power source is AC at this time, the status bit is not set. However, if DC power subsequently returns to the platform, the DC Expired Timer begins running. Refer to WADT_EXP_DC for more details. • The timer returns to its default value of FFFFFFFFh. ***Note:*** Bits in this register only need to be valid for reading when the Main power well is up.

5.1.37 WADT_EXP_AC—Wake Alarm Device Expired Timer – AC Register

Offset Address: 3308–330Bh Attribute: R/W
Default Value: FFFFFFFFh Size: 32-bit

Bit	Description
31:0	**Wake Alarm Device Expired Timer Value for AC Mode (WADT_EXP_AC_VAL):** R/W. This field contains the 32-bit wake alarm device "Expired Timer" value (1 second granularity) for AC power. The timer begins decrementing after switching from DC to AC power, in the case where the WADT_AC timer has already expired while platform was on DC power. This timer only decrements while operating on AC power. So if the power source switches back to DC power, the timer will stop (but not reset). When AC power returns, the timer will again begin decrementing. Upon expiration of this timer: • If on AC power, GPE0_STS.WADT_STS will be set. This status bit being set will generate a host wake if GPE0_EN.WADT_EN is '1'. • Both the AC and DC Expired Timers return to their default value of FFFFFFFFh. ***Note:*** This timer will only begin decrementing under the conditions described above if this field has been configured for something other than its default value of FFFFFFFFh. ***Note:*** Bits in this register only need to be valid for reading when the Main power well is up.

5.1.38 WADT_EXP_DC—Wake Alarm Device Expired Timer: DC Register

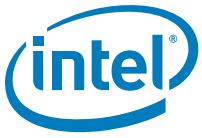
Offset Address: 330C–330Fh Attribute: R/W
Default Value: FFFFFFFFh Size: 32-bit

Bit	Description
31:0	**Wake Alarm Device Expired Timer Value for DC Mode (WADT_EXP_DC_VAL):** R/W. This field contains the 32-bit wake alarm device "Expired Timer" value (1 second granularity) for DC power. The timer begins decrementing after switching from AC to DC power, in the case where the WADT_DC timer has already expired while platform was on AC power. This timer only decrements while operating on DC power. So if the power source switches back to AC power, the timer will stop (but not reset). When DC power returns, the timer will again begin decrementing. Upon expiration of this timer: • If on DC power, GPE0_STS.WADT_STS will be set. This status bit being set will generate a host wake if GPE0_EN.WADT_EN is '1'. • Both the AC and DC Expired Timers return to their default value of FFFFFFFFh. • ***Note:*** This timer will only begin decrementing under the conditions described above if this field has been configured for something other than its default value of FFFFFFFF. ***Note:*** Bits in this register only need to be valid for reading when the Main power well is up.

5.1.39 PRSTS—Power and Reset Status Register

Offset Address: 3310–3313h Attribute: RO, R/WC
Default Value: 05000000h Size: 32-bit

Bit	Description
31:16	Reserved
15	**Power Management Watchdog Timer** — R/WC. This bit is set when the Power Management watchdog timer causes a global reset. This bit is cleared when the software writes it with a 1b.
14:7	Reserved
6	**Intel® Management Engine Watchdog Timer Status** — R/WC. This bit is set when the Intel Management Engine watchdog timer causes a global reset. This bit is cleared when the software writes it with a 1b.



Bit	Description
5	**Wake On LAN Override Wake Status (WOL_OVR_WK_STS)** — R/WC. This bit gets set when all of the following conditions are met: • Integrated LAN Signals a Power Management Event • The system is not in S0 • The "WoL Enable Override" bit is set in configuration space. BIOS can read this status bit to determine this wake source. Software clears this bit by writing a 1 to it.
4	**PRSTS Field 1 —** R/WC. BIOS may program this field.
3	**Intel ME Host Power Down (ME_HOST_PWRDN)** — R/WC. This bit is set when the Intel Management Engine generates a host reset with power down.
2	**Intel ME Host Reset Warm Status (ME_HRST_WARM_STS)** — R/WC. This bit is set when the Intel Management Engine generates a Host reset without power cycling. Software clears this bit by writing a 1 to this bit position.
1	**Intel ME Host Reset Cold Status (ME_HRST_COLD_STS)** — R/WC. This bit is set when the Intel Management Engine generates a Host reset with power cycling. Software clears this bit by writing a 1 to this bit position.
0	**Intel ME WAKE STATUS (ME_WAKE_STS)** — R/WC. This bit is set when the Intel Management Engine generates a Non-Maskable wake event, and is not affected by any other enable bit. When this bit is set, the Host Power Management logic wakes to S0.

5.1.40 CIR3314—Chipset Initialization Register 3314

Offset Address: 3314–3317h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:11	Reserved
10:0	**CIR3314 Field 1**— R/W. BIOS may write to this field.

5.1.41 PM_CFG—Power Management Configuration Register

Offset Address: 3318–331Bh Attribute: R/W
Default Value: 00000020h Size: 32-bit

Bit	Description
31:27	Reserved
26:24	**PM_CFG Field 1 —** R/W. BIOS must program this field to 101b.
23:20	Reserved
19:18	**SLP_SUS# Minimum Assertion Width (SLP_SUS_MIN_ASST_WDTH)**— R/WL. This field indicates the minimum assertion width of the SLP_SUS# signal to guarantee that the SUS power supplies have been fully power cycled. This value may be modified per platform depending on power supply capacitance, board capacitance, power circuits, and so on. Valid values are: 11 = 4 seconds 10 = 1 second 01 = 500 ms 00 = 0 ms (that is, stretching disabled - default) These bits are cleared by RTCRST# assertion. ***Notes:*** 1. This field is RO when the SLP Stretching Policy Lock-Down bit is set. 2. This field is ignored when exiting G3 states if the "Disable SLP Stretching After SUS Well Power Up" bit is set. Unlike with all other SLP_* pin stretching, this disable bit only impacts SLP_SUS# stretching during G3 exit, rather than both G3 exit.

Bit	Description
17:16	**SLP_A# Minimum Assertion Width (SLP_A_MIN_ASST_WDTH)** — R/W. This field indicates the minimum assertion width of the SLP_A# signal to guarantee that the VCCIOIN supplies have been fully power cycled. This value may be modified per platform depending on power supply capacitance, board capacitance, power circuits, and so on. Valid values are: 11 = 2 seconds 10 = 98 ms 01 = 4 seconds 00 = 0 ms (that is, stretching disabled – default) These bits are cleared by RTCRST# assertion. ***Notes:*** 1. This field is RO when the SLP Stretching Policy Lock-Down bit is set. 2. This field is ignored when exiting G3 states if the “Disable SLP Stretching After SUS Well Power Up” bit is set.
15:14	**SLP_LAN# Minimum Assertion Width (SLP_LAN_MIN_ASST_WDTH)** — R/WL. This field indicates the minimum assertion width of the SLP_LAN# signal to guarantee that the PHY power supplies have been fully power cycled. This value may be modified per platform depending on power supply capacitance, board capacitance, power circuits, and so on. Valid values are: 11 = 2 seconds 10 = 50 ms 01 = 1 ms 00 = 0 ms (that is, stretching disabled – default) These bits are cleared by RTCRST# assertion. ***Note:*** This field is RO when the SLP Stretching Policy Lock-Down bit is set.
13:10	Reserved
9:8	**Reset Power Cycle Duration (PWR_CYC_DUR)** — R/WL. This field indicates the minimum time a platform will stay in reset (SLP_S3#, SLP_S4#, SLP_S5# asserted and SLP_A# and SLP_LAN# asserted if applicable) during a host reset with power cycle, host reset with power down or a global reset. The duration programmed in this register takes precedence over the applicable SLP_# stretch timers in these reset scenario. Valid values are: 11 = 1-2 seconds 10 = 2-3 seconds 01 = 3-4 seconds 00 = 4-5 seconds (default) These bits are cleared by RTCRST# assertion. ***Notes:*** 1. This field is RO when the SLP Stretching Policy Lock-Down bit is set. 2. The duration programmed in this register should never be smaller than the stretch duration programmed in the following registers: — GEN_PMCON_3.SLP_S3_MIN_ASST_WDTH — GEN_PMCON_3.SLP_S4_MIN_ASST_WDTH — PM_CFG.SLP_A_MIN_ASST_WDTH — PM_CFG.SLP_LAN_MIN_ASST_WDTH
7:5	Reserved
4	**Host Wireless LAN PHY Power Enable (HOST_WLAN_PP_EN)** - R/W. Set by host software when it desires the WiFi LAN PHY to be powered in Sx power states for Wake Over WiFi (WoWLAN). See SLP_WLAN# for more information. Default = 0b.
3:0	Reserved

5.1.42 CIR3324—Chipset Initialization Register 3324

Offset Address: 3324–3327h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR3324 Field 1** — R/W. BIOS must program this field to 04000000h.

5.1.43 DCIR3340—Chipset Initialization Register 3340

Offset Address: 3340–3343h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:20	Reserved
19:0	**CIR3340 Field 1** — R/W. BIOS may program this register.

5.1.44 CIR3344—Chipset Initialization Register 3344

Offset Address: 3344–3347h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:2	Reserved
1:0	**CIR3344 Field 1** — R/W. BIOS must program this field to 10b.

5.1.45 CIR3348—Chipset Initialization Register 3348

Offset Address: 3348–334Bh Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:8	Reserved
7	**CIR3348 Field 8 —** R/W. BIOS may program this field for PCIe port 8.
6	**CIR3348 Field 7 —** R/W. BIOS may program this field for PCIe port 7.
5	**CIR3348 Field 6 —** R/W. BIOS may program this field for PCIe port 6.
4	**CIR3348 Field 5 —** R/W. BIOS may program this field for PCIe port 5.
3	**CIR3348 Field 4 —** R/W. BIOS may program this field for PCIe port 4.
2	**CIR3348 Field 3 —** R/W. BIOS may program this field for PCIe port 3.
1	**CIR3348 Field 2 —** R/W. BIOS may program this field for PCIe port 2.
0	**CIR3348 Field 1 —** R/W. BIOS may program this field for PCIe port 1.

5.1.46 CIR3350—Chipset Initialization Register 3350

Offset Address: 3350–3353h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:8	Reserved
7	**CIR3350 Field 8 —** R/W. BIOS may program this field for PCIe port 8.
6	**CIR3350 Field 7 —** R/W. BIOS may program this field for PCIe port 7.
5	**CIR3350 Field 6 —** R/W. BIOS may program this field for PCIe port 6.
4	**CIR3350 Field 5 —** R/W. BIOS may program this field for PCIe port 5.

Bit	Description
3	**CIR3350 Field 4 —** R/W. BIOS may program this field for PCIe port 4.
2	**CIR3350 Field 3 —** R/W. BIOS may program this field for PCIe port 3.
1	**CIR3350 Field 2 —** R/W. BIOS may program this field for PCIe port 2.
0	**CIR3350 Field 1 —** R/W. BIOS may program this field for PCIe port 1.

5.1.47 CIR3360—Chipset Initialization Register 3360

Offset Address: 3360–3363h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR3360 Field 1** — R/W. BIOS must program this field to 0001C000h.

5.1.48 CIR3368—Chipset Initialization Register 3368

Offset Address: 3368–336Bh Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR3368 Field 1** — R/W. BIOS may program this register.

5.1.49 CIR3378—Chipset Initialization Register 3378

Offset Address: 3378–337Bh Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR3378 Field 1** — R/W. BIOS may program this register.

5.1.50 CIR337C—Chipset Initialization Register 337C

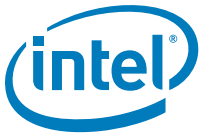
Offset Address: 337C–337Fh Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR337C Field 1** — R/W. BIOS may program this register.

5.1.51 CIR3388—Chipset Initialization Register 3388

Offset Address: 3388–338Bh Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR3388 Field 1** — R/W. BIOS must program this field to 00001000h.



5.1.52 CIR3390—Chipset Initialization Register 3390

Offset Address: 3390–3393h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR3390 Field 1** — R/W. BIOS must program this field to 0001C000h.

5.1.53 CIR33A0—Chipset Initialization Register 33A0

Offset Address: 33A0–33A3h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR33A0 Field 1** — R/W. BIOS must program this field to 00000800h.

5.1.54 CIR33B0—Chipset Initialization Register 33B0

Offset Address: 33B0–33B3h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR33B0 Field 1** — R/W. BIOS must program this field to 00001000h.

5.1.55 CIR33C0—Chipset Initialization Register 33C0

Offset Address: 33C0–33C3h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR33C0 Field 1** — R/W. BIOS may program this register.

5.1.56 PMSYNC_CFG—PMSYNC Configuration

Offset Address: 33C8–33CBh Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:12	Reserved
11	**GPIO_D Pin Selection (GPIO_D_SEL)** — R/W. There are one possible GPIO that this can be routed to the GPIO_D PMSYNC state. This bit must be set as '0b' 0 = GPIO5 (default) 1 = Undefined
10	**GPIO_C Pin Selection (GPIO_C_SEL)** — R/W. There are two possible GPIOs that can be routed to the GPIO_C PMSYNC state. This bit selects between them: 0 = GPIO37 (default) 1 = GPIO4
9	**GPIO_B Pin Selection (GPIO_B_SEL)** — R/W. There are one possible GPIO that this can be routed to the GPIO_B PMSYNC state. This bit must be set as '1b' 0 = Undefined (default) 1 = GPIO37
8	**GPIO_A Pin Selection (GPIO_A_SEL)** — R/W. There are two possible GPIOs that can be routed to the GPIO_A PMSYNC state. This bit selects between them: 0 = GPIO4 (default) 1 = GPIO5
7:0	Reserved

5.1.57 CIR33D0—Chipset Initialization Register 33D0

Offset Address: 33D0–33D3h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR33D0 Field 1** — R/W. BIOS may program this register.

5.1.58 CIR33D4—Chipset Initialization Register 33D4

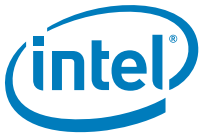
Offset Address: 33D4–33D7h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31	**GPIO_D to PMSYNC Enable (GPIO_D_PMSYNC_EN)** — R/W. 0 = GPIO_D (as selected in RCBA+33C8h) pin state not sent to processor over PMSYNC. 1 = GPIO_D state sent to processor over PMSYNC.
30	**GPIO_C to PMSYNC Enable (GPIO_C_PMSYNC_EN)** — R/W. 0 = GPIO_C (as selected in RCBA+33C8h) pin state not sent to processor over PMSYNC. 1 = GPIO_C state sent to processor over PMSYNC.
29	**GPIO_B to PMSYNC Enable (GPIO_B_PMSYNC_EN)** — R/W. 0 = GPIO_B (as selected in RCBA+33C8h) pin state not sent to processor over PMSYNC. 1 = GPIO_B state sent to processor over PMSYNC.
28	**GPIO_A to PMSYNC Enable (GPIO_A_PMSYNC_EN)** — R/W. 0 = GPIO_A (as selected in RCBA+33C8h) pin state not sent to processor over PMSYNC. 1 = GPIO_A state sent to processor over PMSYNC.
27:0	**CIR33D4 Field 1** — R/W. BIOS may program this register.

5.1.59 RC—RTC Configuration Register

Offset Address: 3400–3403h Attribute: R/W, R/WLO
Default Value: 00000000h Size: 32-bit

Bit	Description
31:5	Reserved
4	**Upper 128 Byte Lock (UL)** — R/WLO. 0 = Bytes not locked. 1 = Bytes 38h–3Fh in the upper 128-byte bank of RTC RAM are locked and cannot be accessed. Writes will be dropped and reads will not return any ensured data. Bit reset on system reset.
3	**Lower 128 Byte Lock (LL)** — R/WLO. 0 = Bytes not locked. 1 = Bytes 38h–3Fh in the lower 128-byte bank of RTC RAM are locked and cannot be accessed. Writes will be dropped and reads will not return any ensured data. Bit reset on system reset.
2	**Upper 128 Byte Enable (UE)** — R/W. 0 = Bytes locked. 1 = The upper 128-byte bank of RTC RAM can be accessed.
1:0	Reserved



5.1.60 HPTC—High Precision Timer Configuration Register

Offset Address: 3404–3407h
Default Value: 00000000h
Attribute: R/W
Size: 32-bit

Bit	Description
31:8	Reserved
7	**Address Enable (AE)** — R/W. 0 = Address disabled. 1 = Intel® Xeon® Processor D-1500 Product Family will decode the High Precision Timer memory address range selected by bits 1:0 below.
6:2	Reserved
1:0	**Address Select (AS)** — R/W. This 2-bit field selects 1 of 4 possible memory address ranges for the High Precision Timer functionality. The encodings are: 00 = FED0_0000h – FED0_03FFh 01 = FED0_1000h – FED0_13FFh 10 = FED0_2000h – FED0_23FFh 11 = FED0_3000h – FED0_33FFh

5.1.61 GCS—General Control and Status Register

Offset Address: 3410–3413h
Default Value: 00000yy0h
(yy = xx0000x0b)
Attribute: R/W, R/WLO
Size: 32-bit

Bit	Description
31:12	Reserved
11:10	**Boot BIOS Straps (BBS)** — R/W. This field determines the destination of accesses to the BIOS memory range. The default values for these bits represent the strap values of GPIO51 (bit 11) at the rising edge of PCH_PWROK and SATA1GP/GPIO19 (bit 10) at the rising edge of PCH_PWROK. **Bits 11:10** — **Description** 00b — LPC 01b — Reserved 10b — Reserved 11b — SPI When SPI or LPC is selected, the range that is decoded is further qualified by other configuration bits described in the respective sections. The value in this field can be overwritten by software as long as the BIOS Interface Lock-Down (bit 0) is not set. Boot BIOS Destination Select to LPC by functional strap or using Boot BIOS Destination Bit will not affect SPI accesses initiated by Intel Management Engine or Integrated GbE LAN.
9	**Server Error Reporting Mode (SERM)** — R/W. 0 = Intel® Xeon® Processor D-1500 Product Family is the final target of all errors. The processor sends a messages to Intel® Xeon® Processor D-1500 Product Family for the purpose of generating NMI. 1 = The processing unit is the final target of all errors from PCI Express and internal messages. In this mode, if Intel® Xeon® Processor D-1500 Product Family detects a fatal, non-fatal, or correctable error internally or its downstream ports, it sends a message to the processor. If Intel® Xeon® Processor D-1500 Product Family receives an ERR_* message from the downstream port, it sends that message to the processing unit.
8:6	Reserved
5	**No Reboot (NR)** — R/W. This bit is set when the "No Reboot" strap (SPKR pin on Intel® Xeon® Processor D-1500 Product Family) is sampled high on PCH_PWROK. This bit may be set or cleared by software if the strap is sampled low but may not override the strap when it indicates "No Reboot". 0 = System will reboot upon the second timeout of the TCO timer. 1 = The TCO timer will count down and generate the SMI# on the first timeout, but will not reboot on the second timeout.

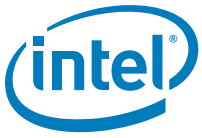
Bit	Description
4	**Alternate Access Mode Enable (AME)** — R/W. 0 = Disabled. 1 = Alternate access read only registers can be written, and write only registers can be read. Before entering a low power state, several registers from powered down parts may need to be saved. In the majority of cases, this is not an issue, as registers have read and write paths. However, several of the ISA compatible registers are either read only or write only. To get data out of write-only registers, and to restore data into read-only registers, Intel® Xeon® Processor D-1500 Product Family implements an alternate access mode. For a list of these registers see Section 3.12.8.
3	**Shutdown Policy Select (SPS)** — R/W. 0 = Intel® Xeon® Processor D-1500 Product Family will drive INIT# in response to the shutdown Vendor Defined Message (VDM). (default) 1 = Intel® Xeon® Processor D-1500 Product Family will treat the shutdown VDM similar to receiving a CF9h I/O write with data value 06h, and will drive PLTRST# active.
2	**Reserved Page Route (RPR)** — R/W. Determines where to send the reserved page registers. These addresses are sent to PCI or LPC for the purpose of generating POST codes. The I/O addresses modified by this field are: 80h, 84h, 85h, 86h, 88h, 8Ch, 8Dh, and 8Eh. 0 = Writes will be forwarded to LPC, shadowed within Intel® Xeon® Processor D-1500 Product Family, and reads will be returned from the internal shadow 1 = Writes will be forwarded to PCI, shadowed within Intel® Xeon® Processor D-1500 Product Family, and reads will be returned from the internal shadow. ***Note:*** if some writes are done to LPC/PCI to these I/O ranges, and then this bit is flipped, such that writes will now go to the other interface, the reads will not return what was last written. Shadowing is performed on each interface. The aliases for these registers, at 90h, 94h, 95h, 96h, 98h, 9Ch, 9Dh, and 9Eh, are always decoded to LPC.
1	Reserved
0	**BIOS Interface Lock-Down (BILD)** — R/WLO. 0 = Disabled. 1 = Prevents BUC.TS (offset 3414, bit 0) and GCS.BBS (offset 3410h, bits 11:10) from being changed. This bit can only be written from 0 to 1 once.

5.1.62 BUC—Backed Up Control Register

Offset Address: 3414h — Attribute: R/W
Default Value: 0000000xb — Size: 8-bit

All bits in this register are in the RTC well and only cleared by RTCRST#.

Bit	Description
7:6	Reserved
5	**LAN Disable** — R/W. 0 = LAN is Enabled 1 = LAN is Disabled. Changing the internal GbE controller from disabled to enabled requires a system reset (write of 0Eh to CF9h (RST_CNT Register)) immediately after clearing the LAN disable bit. A reset is not required if changing the bit from enabled to disabled. This bit is locked by the Function Disable SUS Well Lockdown register. Once locked, this bit cannot be changed by software.
4	**Daylight Savings Override (SDO)** — R/W. 0 = Daylight Savings is Enabled and configurable by software. 1 = The DSE bit in RTC Register B bit[0] is set to Read-only with a value of 0 to disable daylight savings. ***Note:*** System BIOS shall configure this bit accordingly during the boot process before RTC time is initialized.
3:1	**Reserved**



Bit	Description
0	**Top Swap (TS)** — R/W. 0 = Intel® Xeon® Processor D-1500 Product Family will not allow invert the boot block. 1 = Intel® Xeon® Processor D-1500 Product Family will allow boot block invert, for cycles going to the BIOS space. ***Note:*** If Top Swap is enabled (TS = 1b): 1. If booting from SPI, then the BIOS boot block size (BOOT_BLOCK_SIZE) **soft strap** determines if A16, A17, A18, A19 or A20 should be inverted. 2. If booting from LPC (FWH), then the boot-block size is hard-set to 64 KB and only A16 is inverted (soft strap is ignored in this case). 3. If Intel® Xeon® Processor D-1500 Product Family is strapped for Top Swap (GPIO55 is low at rising edge of PCH_PWROK), then this bit **cannot** be cleared by software. The strap jumper should be removed and the system rebooted.

5.1.63 FD—Function Disable Register

Offset Address:	3418–341Bh	Attribute:	R/W
Default Value:	See bit description	Size:	32-bit

When disabling a function, only the configuration space is disabled. Software must ensure that all functionality within a controller that is not desired (such as memory spaces, I/O spaces, and DMA engines) is disabled prior to disabling the function.

When a function is disabled, software must not attempt to re-enable it. A disabled function can only be re-enabled by a platform reset.

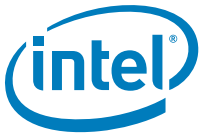
Bit	Description
31:28	Reserved
27	**XHCI Disable (XHD)** — R/W. Default is 0. 0 = The XHCI controller is enabled. 1 = The XHCI controller is disabled.
26	Reserved
25	**Serial ATA Disable 2 (SAD2)** — R/W. Default is 0. 0 = The SATA controller #2 (D31:F5) is enabled. 1 = The SATA controller #2 (D31:F5) is disabled.
24	**Thermal Sensor Registers Disable (TTD)** — R/W. Default is 0. 0 = Thermal Sensor Registers (D31:F6) are enabled. 1 = Thermal Sensor Registers (D31:F6) are disabled.
23	**PCI Express* 8 Disable (PE8D)** — R/W. Default is 0. When disabled, the link for this port is put into the "link down" state. 0 = PCI Express* port #8 is enabled. 1 = PCI Express port #8 is disabled.
22	**PCI Express 7 Disable (PE7D)** — R/W. Default is 0. When disabled, the link for this port is put into the link down state. 0 = PCI Express port #7 is enabled. 1 = PCI Express port #7 is disabled.
21	**PCI Express* 6 Disable (PE6D)** — R/W. Default is 0. When disabled, the link for this port is put into the "link down" state. 0 = PCI Express* port #6 is enabled. 1 = PCI Express port #6 is disabled.
20	**PCI Express 5 Disable (PE5D)** — R/W. Default is 0. When disabled, the link for this port is put into the link down state. 0 = PCI Express port #5 is enabled. 1 = PCI Express port #5 is disabled.
19	**PCI Express 4 Disable (PE4D)** — R/W. Default is 0. When disabled, the link for this port is put into the "link down" state. 0 = PCI Express port #4 is enabled. 1 = PCI Express port #4 is disabled. ***Note:*** This bit must be set when Port 1 is configured as a x4.

Bit	Description
18	**PCI Express 3 Disable (PE3D)** — R/W. Default is 0. When disabled, the link for this port is put into the link down state. 0 = PCI Express port #3 is enabled. 1 = PCI Express port #3 is disabled. ***Note:*** This bit must be set when Port 1 is configured as a x4.
17	**PCI Express* 2 Disable (PE2D)** — R/W. Default is 0. When disabled, the link for this port is put into the link down state. 0 = PCI Express port #2 is enabled. 1 = PCI Express port #2 is disabled. ***Note:*** This bit must be set when Port 1 is configured as a x4 or a x2.
16	**PCI Express 1 Disable (PE1D)** — R/W. Default is 0. When disabled, the link for this port is put into the link down state. 0 = PCI Express port #1 is enabled. 1 = PCI Express port #1 is disabled.
15	**EHCI #1 Disable (EHCI1D)** — R/W. Default is 0. 0 = The EHCI #1 is enabled. 1 = The EHCI #1 is disabled.
14	**LPC Bridge Disable (LBD)** — R/W. Default is 0. 0 = The LPC bridge is enabled. 1 = The LPC bridge is disabled. Unlike the other disables in this register, the following additional spaces will no longer be decoded by the LPC bridge: • Memory cycles below 16 MB (1000000h) • I/O cycles below 64 KB (10000h) • The Internal I/OxAPIC at FEC0_0000 to FECF_FFFF Memory cycle in the LPC BIOS range below 4 GB will still be decoded when this bit is set; however, the aliases at the top of 1 MB (the E and F segment) no longer will be decoded.
13	**EHCI #2 Disable (EHCI2D)** — R/W. Default is 0. 0 = The EHCI #2 is enabled. 1 = The EHCI #2 is disabled.
12:5	Reserved
4	**Intel® High Definition Audio Disable (HDAD)** — R/W. Default is 0. 0 = The Intel High Definition Audio controller is enabled. 1 = The Intel High Definition Audio controller is disabled and its PCI configuration space is not accessible. Note: HD Audio is not supported. This bit will be set to 1.
3	**SMBus Disable (SD)** — R/W. Default is 0. 0 = The SMBus controller is enabled. 1 = The SMBus controller is disabled. Setting this bit only disables the PCI configuration space.
2	**Serial ATA Disable 1 (SAD1)** — R/W. Default is 0. 0 = The SATA controller #1 (D31:F2) is enabled. 1 = The SATA controller #1 (D31:F2) is disabled.
1	Reserved.
0	BIOS must program this field to 1b.

5.1.64 CG—Clock Gating Register

Offset Address: 341C–341Fh Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31	**Legacy (LPC) Dynamic Clock Gate Enable** — R/W. 0 = Legacy Dynamic Clock Gating is Disabled 1 = Legacy Dynamic Clock Gating is Enabled
30:24	Reserved
23	**LAN Static Clock Gating Enable (LANSCGE)** — R/W. 0 = LAN Static Clock Gating is Disabled 1 = LAN Static Clock Gating is Enabled when the LAN Disable bit is set in the Backed Up Control RTC register.



Bit	Description
22:17	Reserved
16	**PCI Dynamic Gate Enable** — R/W. 0 = PCI Dynamic Gating is Disabled 1 = PCI Dynamic Gating is Enabled
15:6	Reserved
5	**SMBus Clock Gating Enable (SMBCGEN)** — R/W. 0 = SMBus Clock Gating is Disabled. 1 = SMBus Clock Gating is Enabled. ***Note:*** Setting this bit will also clock gate all the TCO logic functionality.
4:0	Reserved

5.1.65 DISPBDF—Display Bus, Device and Function Initialization Register

Offset Address: 3424–3427h Attribute: R/W
Default Value: 00040010h Size: 32-bit

Bit	Description
31:19	Reserved.
18:16	**Display Target Block (DTB)** — R/W. The Target BLK field that Intel® Xeon® Processor D-1500 Product Family South Display controller should use when sending RAVDM messages to the processor. BIOS must program this field to 110h.
15:8	**Display Bus Number (DBN)** — R/W. The bus number of the Display in the processor. BIOS must program this field to 0h.
7:3	**Display Device Number (DDN)** — R/W. The device number of the Display in the processor. BIOS must program this field to 2h.
2:0	**Display Function Number (DFN)** — R/W. The function number of the Display in the processor. BIOS must program this field to 0h.

5.1.66 FD2—Function Disable 2 Register

Offset Address: 3428–342Bh Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:5	Reserved
4	**KT Disable (KTD)** —R/W. Default is 0. 0 = Keyboard Text controller (D22:F3) is enabled. 1 = Keyboard Text controller (D22:F3) is Disabled
3	**IDE-R Disable (IRERD)** —R/W. Default is 0. 0 = IDE Redirect controller (D22:F2) is Enabled. 1 = IDE Redirect controller (D22:F2) is Disabled.
2	**Intel® MEI #2 Disable (MEI2D)** —R/W. Default is 0. 0 = Intel MEI controller #2 (D22:F1) is enabled. 1 = Intel MEI controller #2 (D22:F1) is disabled.
1	**Intel MEI #1 Disable (MEI1D)** —R/W. Default is 0. 0 = Intel MEI controller #1 (D22:F0) is enabled. 1 = Intel MEI controller #1 (D22:F0) is disabled.
0	**Display BDF Enable (DBDFEN)** —R/W. Default is 0.

5.1.67 CIR3A28—Chipset Initialization Register 3A28

Offset Address: 3A28–3A2Bh Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR3A28 Field 1** — R/W. BIOS must program this field to 01010000h.

5.1.68 CIR3A2C—Chipset Initialization Register 3A2C

Offset Address: 3A2C–3A2Fh Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR3A2C Field 1** — R/W. BIOS must program this field to 01010404h.

5.1.69 CIR3A6C—Chipset Initialization Register 3A6C

Offset Address: 3A6C–3A6Fh Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR3A6C Field 1** — R/W. BIOS must program this field to 00000001h.

5.1.70 CIR3A80—Chipset Initialization Register 3A80

Offset Address: 3A80–3A83h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	**CIR3A80 Field 1** — R/W. BIOS may program this register.

5.1.71 CIR3A84—Chipset Initialization Register 3A84

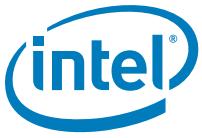
Offset Address: 3A84–3A87h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:25	Reserved
24	**CIR3A84 Field 3** — R/W. BIOS may program this field.
23:19	Reserved
18	**CIR3A84 Field 2** — R/W. BIOS may program this field.
17:16	Reserved
15:0	**CIR3A84 Field 1** — R/W. BIOS may program this register.

5.1.72 CIR3A88—Chipset Initialization Register 3A88

Offset Address: 3A88–3A8Ch Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:1	Reserved
0	**CIR3A88 Field 1** — R/W. BIOS may program this field.



5.2 Thermal Configuration Registers

Note: All registers here are an offset of TBARB (see Section 16.1.19).

Table 5-2. Thermal Initialization Registers

Offset	Mnemonic	Register Name	Default	Attribute
C0h-C3h	TIRC0	Thermal Initialization Register C0	00000000h	R/W
C4h-C7h	TIRC4	Thermal Initialization Register C4	00000000h	R/W
C8h-CBh	TIRC8	Thermal Initialization Register C8	00000000h	R/W
CCh-CFh	TIRCC	Thermal Initialization Register CC	00000000h	R/W
D0h-D3h	TIRD0	Thermal Initialization Register D0	00000000h	R/W
E0h-E3h	TIRE0	Thermal Initialization Register E0	00000000h	R/W
F0h-F3h	TIRF0	Thermal Initialization Register F0	00000000h	R/W

5.2.1 TIRC0—Thermal Initialization Register C0

Offset Address: C0–C3h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	R/W. BIOS must program this field to 8000390Bh. No other values are supported.

5.2.2 TIRC4—Thermal Initialization Register C4

Offset Address: C4–C7h Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	R/W. BIOS must program this field to C11F0201h. No other values are supported.

5.2.3 TIRC8—Thermal Initialization Register C8

Offset Address: C8–CBh Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	R/W. BIOS must program this field to 05800000h. No other values are supported.

5.2.4 TIRCC—Thermal Initialization Register CC

Offset Address: CC–CFh Attribute: R/W
Default Value: 00000000h Size: 32-bit

Bit	Description
31:0	R/W. BIOS must program this field to 0000C000h. No other values are supported.

5.2.5 TIRD0—Thermal Initialization Register D0

Offset Address: D0–D3h
Attribute: R/W
Default Value: 00000000h
Size: 32-bit

Bit	Description
31:0	R/W. BIOS must program this field to 00000320h. No other values are supported.

5.2.6 TIRE0—Thermal Initialization Register E0

Offset Address: E0–E3h
Attribute: R/W
Default Value: 00000000h
Size: 32-bit

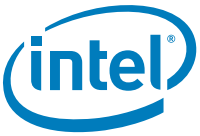
Bit	Description
31:0	R/W. BIOS must program this field to 80001E4Fh. No other values are supported.

5.2.7 TIRF0—Thermal Initialization Register F0

Offset Address: F0–F3h
Attribute: R/W
Default Value: 00000000h
Size: 32-bit

Bit	Description
31:0	R/W. BIOS must program this field to 00000003h. No other values are supported.

§



6 Gigabit LAN Configuration Registers

6.1 Gigabit LAN Configuration Registers (Gigabit LAN—D25:F0)

Note: Register address locations that are not shown in Table 6-1 should be treated as Reserved. All GbE registers are located in the VccIOIN power well.

Table 6-1. Gigabit LAN Configuration Registers Address Map (Gigabit LAN—D25:F0) (Sheet 1 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
00h–01h	VID	Vendor Identification	8086h	RO
02h–03h	DID	Device Identification	See register description	RO
04h–05h	PCICMD	PCI Command	0000h	R/W, RO
06h–07h	PCISTS	PCI Status	0010h	R/WC, RO
08h	RID	Revision Identification	See register description	RO
09h–0Bh	CC	Class Code	020000h	RO
0Ch	CLS	Cache Line Size	00h	R/W
0Dh	PLT	Primary Latency Timer	00h	RO
0Eh	HEADTYP	Header Type	00h	RO
10h–13h	MBARA	Memory Base Address A	00000000h	R/W, RO
14h–17h	MBARB	Memory Base Address B	00000000h	R/W, RO
18h–1Bh	MBARC	Memory Base Address C	00000001h	R/W, RO
2Ch–2Dh	SVID	Subsystem Vendor ID	See register description	RO
2Eh–2Fh	SID	Subsystem ID	See register description	RO
30h–33h	ERBA	Expansion ROM Base Address	See register description	RO
34h	CAPP	Capabilities List Pointer	C8h	RO
3Ch–3Dh	INTR	Interrupt Information	See register description	R/W, RO
3Eh–3Fh	MLMG	Maximum Latency / Minimum Grant	0000h	RO
A0h–A3h	STCL	System Time Capture Low	00000000h	RO
A4h–A7h	STCH	System Time Capture High	00000000h	RO
A8h–ABh	LTR	Latency Tolerance Reporting	00000000h	R/W
C8h–C9h	CLIST1	Capabilities List 1	D001h	RO
CAh–CBh	PMC	PCI Power Management Capability	See register description	RO
CCh–CDh	PMCS	PCI Power Management Control and Status	See register description	R/WC, R/W, RO
CFh	DR	Data Register	See register description	RO
D0h–D1h	CLIST2	Capabilities List 2	E005h	R/WO, RO

Table 6-1. Gigabit LAN Configuration Registers Address Map (Gigabit LAN—D25:F0) (Sheet 2 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
D2h–D3h	MCTL	Message Control	0080h	R/W, RO
D4h–D7h	MADDL	Message Address Low	See register description	R/W
D8h–dBh	MADDH	Message Address High	See register description	R/W
DCh–DDh	MDAT	Message Data	See register description	R/W
E0h–E1h	FLRCAP	Function Level Reset Capability	0009h	RO
E2h–E3h	FLRCLV	Function Level Reset Capability Length and Value	See register description	R/WO, RO
E4h–E5h	DEVCTRL	Device Control	0000h	R/W, RO

6.1.1 VID—Vendor Identification Register (Gigabit LAN—D25:F0)

Address Offset: 00h–01h
Attribute: RO
Default Value: 8086h
Size: 16 bits

Bit	Description
15:0	**Vendor ID** — RO. This is a 16-bit value assigned to Intel. The field may be auto-loaded from the NVM at address 0Dh during init time depending on the "Load Vendor/Device ID" bit field in NVM word 0Ah with a default value of 8086h.

6.1.2 DID—Device Identification Register (Gigabit LAN—D25:F0)

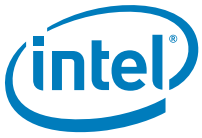
Address Offset: 02h–03h
Attribute: RO
Default Value: See bit description
Size: 16 bits

Bit	Description
15:0	**Device ID** — RO. This is a 16-bit value assigned to Intel® Xeon® Processor D-1500 Product Family Gigabit LAN controller. The field may be auto-loaded from the NVM word 0Dh during initialization time depending on the "Load Vendor/Device ID" bit field in NVM word 0Ah.

6.1.3 PCICMD—PCI Command Register (Gigabit LAN—D25:F0)

Address Offset: 04h–05h
Attribute: R/W, RO
Default Value: 0000h
Size: 16 bits

Bit	Description
15:11	Reserved
10	**Interrupt Disable** — R/W. This disables pin-based INTx# interrupts on enabled Hot-Plug and power management events. This bit has no effect on MSI operation. 0 = Internal INTx# messages are generated if there is an interrupt for Hot-Plug or power management and MSI is not enabled. 1 = Internal INTx# messages will not be generated. This bit does not affect interrupt forwarding from devices connected to the root port. Assert_INTx and Deassert_INTx messages will still be forwarded to the internal interrupt controllers if this bit is set.
9	Fast Back to Back Enable (FBE) — RO. Hardwired to 0.
8	**SERR# Enable (SEE)** — R/W. 0 = Disable 1 = Enables the Gb LAN controller to generate an SERR# message when PSTS.SSE is set.



Bit	Description
7	**Wait Cycle Control (WCC)** — RO. Hardwired to 0.
6	**Parity Error Response (PER)** — R/W. 0 = Disable. 1 = Indicates that the device is capable of reporting parity errors as a master on the backbone.
5	Palette Snoop Enable (PSE) — RO. Hardwired to 0.
4	Postable Memory Write Enable (PMWE) — RO. Hardwired to 0.
3	**Special Cycle Enable (SCE)** — RO. Hardwired to 0.
2	**Bus Master Enable (BME)** — R/W. 0 = Disable. All cycles from the device are master aborted 1 = Enable. Allows the root port to forward cycles onto the backbone from a Gigabit LAN* device.
1	**Memory Space Enable (MSE)** — R/W. 0 = Disable. Memory cycles within the range specified by the memory base and limit registers are master aborted on the backbone. 1 = Enable. Allows memory cycles within the range specified by the memory base and limit registers can be forwarded to the Gigabit LAN device.
0	**I/O Space Enable (IOSE)** — R/W. This bit controls access to the I/O space registers. 0 = Disable. I/O cycles within the range specified by the I/O base and limit registers are master aborted on the backbone. 1 = Enable. Allows I/O cycles within the range specified by the I/O base and limit registers can be forwarded to the Gigabit LAN device.

6.1.4 PCISTS—PCI Status Register (Gigabit LAN—D25:F0)

Address Offset: 06h–07h
Attribute: R/WC, RO
Default Value: 0010h
Size: 16 bits

Bit	Description
15	**Detected Parity Error (DPE)** — R/WC. 0 = No parity error detected. 1 = Set when the Gb LAN controller receives a command or data from the backbone with a parity error. This is set even if PCIMD.PER (D25:F0, bit 6) is not set.
14	**Signaled System Error (SSE)** — R/WC. 0 = No system error signaled. 1 = Set when the Gb LAN controller signals a system error to the internal SERR# logic.
13	**Received Master Abort (RMA)** — R/WC. 0 = Root port has not received a completion with unsupported request status from the backbone. 1 = Set when the GbE LAN controller receives a completion with unsupported request status from the backbone.
12	**Received Target Abort (RTA)** — R/WC. 0 = Root port has not received a completion with completer abort from the backbone. 1 = Set when the Gb LAN controller receives a completion with completer abort from the backbone.
11	**Signaled Target Abort (STA)** — R/WC. 0 = No target abort received. 1 = Set whenever the Gb LAN controller forwards a target abort received from the downstream device onto the backbone.
10:9	**DEVSEL# Timing Status (DEV_STS)** — RO. Hardwired to 0.
8	**Master Data Parity Error Detected (DPED)** — R/WC. 0 = No data parity error received. 1 = Set when the Gb LAN Controller receives a completion with a data parity error on the backbone and PCIMD.PER (D25:F0, bit 6) is set.
7	Fast Back to Back Capable (FB2BC) — RO. Hardwired to 0.
6	Reserved
5	66 MHz Capable — RO. Hardwired to 0.
4	Capabilities List — RO. Hardwired to 1. Indicates the presence of a capabilities list.

Bit	Description
3	Interrupt Status — RO. Indicates status of Hot-Plug and power management interrupts on the root port that result in INTx# message generation. 0 = Interrupt is de-asserted. 1 = Interrupt is asserted. This bit is not set if MSI is enabled. If MSI is not enabled, this bit is set regardless of the state of PCICMD.Interrupt Disable bit (D25:F0:04h:bit 10).
2:0	Reserved

6.1.5 RID—Revision Identification Register (Gigabit LAN—D25:F0)

Offset Address: 08h — Attribute: RO
Default Value: See bit description — Size: 8 bits

Bit	Description
7:0	**Revision ID** — RO. This field indicates the device specific revision identifier.

6.1.6 CC—Class Code Register (Gigabit LAN—D25:F0)

Address Offset: 09h–0Bh — Attribute: RO
Default Value: 020000h — Size: 24 bits

Bit	Description
23:0	**Class Code**— RO. Identifies the device as an Ethernet Adapter. 020000h = Ethernet Adapter.

6.1.7 CLS—Cache Line Size Register (Gigabit LAN—D25:F0)

Address Offset: 0Ch — Attribute: R/W
Default Value: 00h — Size: 8 bits

Bit	Description
7:0	**Cache Line Size** — R/W. This field is implemented by PCI devices as a read write field for legacy compatibility purposes but has no impact on any device functionality.

6.1.8 PLT—Primary Latency Timer Register (Gigabit LAN—D25:F0)

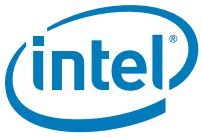
Address Offset: 0Dh — Attribute: RO
Default Value: 00h — Size: 8 bits

Bit	Description
7:0	Latency Timer (LT) — RO. Hardwired to 0.

6.1.9 HEADTYP—Header Type Register (Gigabit LAN—D25:F0)

Address Offset: 0Eh — Attribute: RO
Default Value: 00h — Size: 8 bits

Bit	Description
7:0	**Header Type (HT)** — RO. 00h = Indicates this is a single function device.



6.1.10 MBARA—Memory Base Address Register A (Gigabit LAN—D25:F0)

Address Offset: 10h–13h
Default Value: 00000000h
Attribute: R/W, RO
Size: 32 bits

The internal CSR registers and memories are accessed as direct memory mapped offsets from the base address register. SW may only access whole DWord at a time.

Bit	Description
31:17	**Base Address (BA) — R/W**. Software programs this field with the base address of this region.
16:4	**Memory Size (MSIZE) —** RO. Memory size is 128 KB.
3	**Prefetchable Memory (PM)** — RO. The GbE LAN controller does not implement prefetchable memory.
2:1	**Memory Type (MT)** — RO. Clear to 00b indicating a 32 bit BAR.
0	**Memory / IO Space (MIOS)** — RO. Clear to 0 indicating a Memory Space BAR.

6.1.11 MBARB—Memory Base Address Register B (Gigabit LAN—D25:F0)

Address Offset: 14h–17h
Default Value: 00000000h
Attribute: R/W, RO
Size: 32 bits

The internal registers that are used to access the LAN Space in the External FLASH device. Access to these registers are direct memory mapped offsets from the base address register. Software may only access a DWord at a time.

Bit	Description
31:12	**Base Address (BA) — R/W**. Software programs this field with the base address of this region.
11:4	**Memory Size (MSIZE) —** RO. Memory size is 4 KB.
3	**Prefetchable Memory (PM)** — RO. Clear to 0b indicating the Gb LAN controller does not implement prefetchable memory.
2:1	**Memory Type (MT)** — RO. Clear to 00b indicating a 32 bit BAR.
0	**Memory / IO Space (MIOS)** — RO. Clear to 0 indicating a Memory Space BAR.

6.1.12 MBARC—Memory Base Address Register C (Gigabit LAN—D25:F0)

Address Offset: 18h–1Bh
Default Value: 00000001h
Attribute: R/W, RO
Size: 32 bits

Internal registers, and memories, can be accessed using I/O operations. There are two 4 Byte registers in the I/O mapping window: Addr Reg and Data Reg. Software may only access a DWord at a time.

Bit	Description
31:5	**Base Address (BA) — R/W**. Software programs this field with the base address of this region.
4:1	**I/O Size (IOSIZE)** — RO. I/O space size is 32 Bytes.
0	**Memory / I/O Space (MIOS)** — RO. Set to 1 indicating an I/O Space BAR.

6.1.13 SVID—Subsystem Vendor ID Register (Gigabit LAN—D25:F0)

Address Offset: 2Ch–2Dh
Attribute: RO
Default Value: See bit description
Size: 16 bits

Bit	Description
15:0	**Subsystem Vendor ID (SVID)** — RO. This value may be loaded automatically from the NVM Word 0Ch upon power up or reset depending on the "Load Subsystem ID" bit field in NVM word 0Ah. A value of 8086h is default for this field upon power up if the NVM does not respond or is not programmed. All functions are initialized to the same value.

6.1.14 SID—Subsystem ID Register (Gigabit LAN—D25:F0)

Address Offset: 2Eh–2Fh
Attribute: RO
Default Value: See bit description
Size: 16 bits

Bit	Description
15:0	**Subsystem ID (SID)** — RO. This value may be loaded automatically from the NVM Word 0Bh upon power up or reset depending on the "Load Subsystem ID" bit field in NVM word 0Ah with a default value of 0000h. This value is loadable from NVM word location 0Ah.

6.1.15 ERBA—Expansion ROM Base Address Register (Gigabit LAN—D25:F0)

Address Offset: 30h–33h
Attribute: RO
Default Value: See bit description
Size: 32 bits

Bit	Description
31:0	**Expansion ROM Base Address (ERBA)** — RO. This register is used to define the address and size information for boot-time access to the optional FLASH memory. If no Flash memory exists, this register reports 00000000h.

6.1.16 CAPP—Capabilities List Pointer Register (Gigabit LAN—D25:F0)

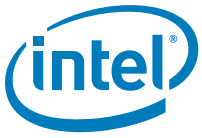
Address Offset: 34h
Attribute: RO
Default Value: C8h
Size: 8 bits

Bit	Description
7:0	**Capabilities Pointer (PTR)** — RO. Indicates that the pointer for the first entry in the capabilities list is at C8h in configuration space.

6.1.17 INTR—Interrupt Information Register (Gigabit LAN—D25:F0)

Address Offset: 3Ch–3Dh
Attribute: R/W, RO
Default Value: 0100h
Size: 16 bits
Function Level Reset: No

Bit	Description
15:8	**Interrupt Pin (IPIN)** — RO. Indicates the interrupt pin driven by the GbE LAN controller. 01h = The GbE LAN controller implements legacy interrupts on INTA.
7:0	**Interrupt Line (ILINE)** — R/W. Default = 00h. Software written value to indicate which interrupt line (vector) the interrupt is connected to. No hardware action is taken on this register.



6.1.18 MLMG—Maximum Latency / Minimum Grant Register (Gigabit LAN—D25:F0)

Address Offset: 3Eh–3Fh Attribute: RO
Default Value: 0000h Size: 16 bits

Bit	Description
7:0	Maximum Latency/Minimum Grant (MLMG) — RO. Not used. Hardwired to 00h.

6.1.19 STCL—System Time Control Low Register (Gigabit LAN—D25:F0)

Address Offset: A0h–A3h Attribute: RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:0	**System Time Control Low (STCL)** — RO. Lower 32 bits of the system time capture used for audio stream synchronization.

6.1.20 STCH—System Time Control High Register (Gigabit LAN—D25:F0)

Address Offset: A4h–A7h Attribute: RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:0	**System Time Control High (STCH)** — RO. Upper 32 bits of the system time capture used for audio stream synchronization.

6.1.21 LTRCAP—System Time Control High Register (Gigabit LAN—D25:F0)

Address Offset: A8h–ABh Attribute: R/W
Default Value: 00000000h Size: 32 bits

Bit	Description
31:29	Reserved
28:26	**Maximum Non-Snoop Latency Scale (MNSLS)** — R/W. Provides a scale for the value contained within the Maximum Non-Snoop Latency Value field. 000b = Value times 1 ns 001b = Value times 32 ns 010b = Value times 1,024 ns 011b = Value times 32,768 ns 100b = Value times 1,048,576 ns 101b = Value times 33,554,432 ns 110b-111b – Reserved
25:16	**Maximum Non-Snoop Latency (MNSL)** — R/W. Specifies the maximum non-snoop latency that a device is permitted to request. Software should set this to the platform's maximum supported latency or less. This field is also an indicator of the platforms maximum latency, should an endpoint send up LTR Latency Values with the Requirement bit not set.
15:13	Reserved

Bit	Description
12:10	**Maximum Snoop Latency Scale (MSLS)** — R/W. Provides a scale for the value contained within the Maximum Snoop Latency Value field. 000b = Value times 1 ns 001b = Value times 32 ns 010b = Value times 1,024 ns 011b = Value times 32,768 ns 100b = Value times 1,048,576 ns 101b = Value times 33,554,432 ns 110b-111b – Reserved
9:0	**Maximum Snoop Latency (MSL)** — R/W. Specifies the maximum snoop latency that a device is permitted to request. Software should set this to the platform's maximum supported latency or less. This field is also an indicator of the platforms maximum latency, should an endpoint send up LTR Latency Values with the Requirement bit not set.

6.1.22 CLIST1—Capabilities List Register 1 (Gigabit LAN—D25:F0)

Address Offset: C8h–C9h Attribute: RO
Default Value: D001h Size: 16 bits

Bit	Description
15:8	**Next Capability (NEXT)** — RO. Value of D0h indicates the location of the next pointer.
7:0	**Capability ID (CID)** — RO. Indicates the linked list item is a PCI Power Management Register.

6.1.23 PMC—PCI Power Management Capabilities Register (Gigabit LAN—D25:F0)

Address Offset: CAh–CBh Attribute: RO
Default Value: See bit descriptions Size: 16 bits
Function Level Reset: No (Bits 15:11 only)

Bit	Description
15:11	**PME_Support (PMES)** — RO. This five-bit field indicates the power states in which the function may assert PME#. It depend on PM Ena and AUX-PWR bits in word 0Ah in the NVM: **Condition** / **Functionality** / **Value** PM Ena=0 / No PME at all states / 0000b PM Ena & AUX-PWR=0 / PME at D0 and D3hot / 01001b PM Ena & AUX-PWR=1 / PME at D0, D3hot and D3cold / 11001b These bits are not reset by Function Level Reset.
10	**D2_Support (D2S)** — RO. The D2 state is not supported.
9	**D1_Support (D1S)** — RO. The D1 state is not supported.
8:6	**Aux_Current (AC)** — RO. Required current defined in the Data Register.
5	**Device Specific Initialization (DSI)** — RO. Set to 1. The GbE LAN Controller requires its device driver to be executed following transition to the D0 un-initialized state.
4	Reserved
3	PME Clock (PMEC) — RO. Hardwired to 0.
2:0	**Version (VS)** — RO. Hardwired to 010b to indicate support for *Revision 1.1 of the PCI Power Management Specification*.

6.1.24 PMCS—PCI Power Management Control and Status Register (Gigabit LAN—D25:F0)

Address Offset: CCh–CDh
Attribute: R/WC, R/W, RO
Default Value: See bit description
Size: 16 bits
Function Level Reset: No (Bit 8 only)

Bit	Description
15	**PME Status (PMES)** — R/WC. This bit is set to 1 when the function detects a wake-up event independent of the state of the PMEE bit. Writing a 1 will clear this bit.
14:13	**Data Scale (DSC)** — RO. This field indicates the scaling factor to be used when interpreting the value of the Data register. For the GbE LAN and common functions this field equals 01b (indicating 0.1 watt units) if the PM is enabled in the NVM, and the Data_Select field is set to 0, 3, 4, 7, (or 8 for Function 0). Else it equals 00b. For the manageability functions this field equals 10b (indicating 0.01 watt units) if the PM is enabled in the NVM, and the Data_Select field is set to 0, 3, 4, 7. Else it equals 00b.
12:9	**Data Select (DSL)** — R/W. This four-bit field is used to select which data is to be reported through the Data register (offset CFh) and Data_Scale field. These bits are writeable only when the Power Management is enabled using NVM. 0h = D0 Power Consumption 3h = D3 Power Consumption 4h = D0 Power Dissipation 7h = D3 Power Dissipation 8h = Common Power All other values are reserved.
8	**PME Enable (PMEE)** — R/W. If Power Management is enabled in the NVM, writing a 1 to this register will enable Wakeup. If Power Management is disabled in the NVM, writing a 1 to this bit has no affect, and will not set the bit to 1. This bit is not reset by Function Level Reset.
7:4	Reserved – Returns a value of 0000.
3	**No Soft Reset (NSR)** — RO. Defines if the device executed internal reset on the transition to D0. the LAN controller always reports 0 in this field.
2	Reserved – Returns a value of 0b.
1:0	**Power State (PS)** — R/W. This field is used both to determine the current power state of the GbE LAN Controller and to set a new power state. The values are: 00 = D0 state (default) 01 = Ignored 10 = Ignored 11 = D3 state (Power Management must be enabled in the NVM or this cycle will be ignored).

6.1.25 DR—Data Register (Gigabit LAN—D25:F0)

Address Offset: CFh
Attribute: RO
Default Value: See bit description
Size: 8 bits

Bit	Description
7:0	**Reported Data (RD)** — RO. This register is used to report power consumption and heat dissipation. This register is controlled by the Data_Select field in the PMCS (Offset CCh, bits 12:9), and the power scale is reported in the Data_Scale field in the PMCS (Offset CCh, bits 14:13). The data of this field is loaded from the NVM if PM is enabled in the NVM or with a default value of 00h otherwise.

6.1.26 CLIST2—Capabilities List Register 2 (Gigabit LAN—D25:F0)

Address Offset: D0h–D1h
Attribute: R/WO, RO
Default Value: E005h
Size: 16 bits
Function Level Reset: No (Bits 15:8 only)

Bit	Description
15:8	**Next Capability (NEXT)** — R/WO. Value of E0h points to the Function Level Reset capability structure. These bits are not reset by Function Level Reset.
7:0	**Capability ID (CID)** — RO. Indicates the linked list item is a Message Signaled Interrupt Register.

6.1.27 MCTL—Message Control Register (Gigabit LAN—D25:F0)

Address Offset: D2h–D3h
Attribute: R/W, RO
Default Value: 0080h
Size: 16 bits

Bit	Description
15:8	Reserved
7	**64-bit Capable (CID)** — RO. Set to 1 to indicate that the GbE LAN Controller is capable of generating 64-bit message addresses.
6:4	**Multiple Message Enable (MME)** — RO. Returns 000b to indicate that the GbE LAN controller only supports a single message.
3:1	**Multiple Message Capable (MMC)** — RO. The GbE LAN controller does not support multiple messages.
0	**MSI Enable (MSIE)** — R/W. 0 = MSI generation is disabled. 1 = The Gb LAN controller will generate MSI for interrupt assertion instead of INTx signaling.

6.1.28 MADDL—Message Address Low Register (Gigabit LAN—D25:F0)

Address Offset: D4h–D7h
Attribute: R/W
Default Value: See bit description
Size: 32 bits

Bit	Description
31:0	**Message Address Low (MADDL)** — R/W. Written by the system to indicate the lower 32 bits of the address to use for the MSI memory write transaction. The lower two bits will always return 0 regardless of the write operation.

6.1.29 MADDH—Message Address High Register (Gigabit LAN—D25:F0)

Address Offset: D8h–dBh
Attribute: R/W
Default Value: See bit description
Size: 32 bits

Bit	Description
31:0	**Message Address High (MADDH)** — R/W. Written by the system to indicate the upper 32 bits of the address to use for the MSI memory write transaction.

6.1.30 MDAT—Message Data Register (Gigabit LAN—D25:F0)

Address Offset: DCh–DDh
Attribute: R/W
Default Value: See bit description
Size: 16 bits

Bit	Description
31:0	**Message Data (MDAT)** — R/W. Written by the system to indicate the lower 16 bits of the data written in the MSI memory write DWord transaction. The upper 16 bits of the transaction are written as 0000h.

6.1.31 FLRCAP—Function Level Reset Capability (Gigabit LAN—D25:F0)

Address Offset: E0h–E1h
Attribute: RO
Default Value: 0009h
Size: 16 bits

Bit	Description
15:8	**Next Pointer** — RO. This field provides an offset to the next capability item in the capability list. The value of 00h indicates the last item in the list.
7:0	**Capability ID** — RO. The value of this field depends on the FLRCSSEL bit. 13h = If FLRCSSEL = 0 09h = If FLRCSSEL = 1, indicating vendor specific capability. FLRCSSEL is located at RCBA + 3410(bit 12). See Chapter 10-Chipset Configuration Registers.

6.1.32 FLRCLV—Function Level Reset Capability Length and Version Register (Gigabit LAN—D25:F0)

Address Offset: E2h–E3h
Attribute: R/WO, RO
Default Value: See Description.
Size: 16 bits
Function Level Reset: No (Bits 9:8 Only When FLRCSSEL = 0)

When FLRCSSEL = 0, this register is defined as follows:

Bit	Description
15:10	Reserved
9	**Function Level Reset Capability** — R/WO. 1 = Support for Function Level Reset. This bit is not reset by Function Level Reset.
8	**TXP Capability** — R/WO. 1 = Indicates support for the Transactions Pending (TXP) bit. TXP must be supported if FLR is supported.
7:0	**Capability Length** — RO. The value of this field indicates the number of bytes of the vendor specific capability as require by the PCI specification. It has the value of 06h for the Function Level Reset capability.

When FLRCSSEL = 1, this register is defined as follows:

Bit	Description
15:12	**Vendor Specific Capability ID** — RO. A value of 2h in this field identifies this capability as Function Level Reset.
11:8	**Capability Version**— RO. The value of this field indicates the version of the Function Level Reset Capability. Default is 0h.
7:0	**Capability Length** — RO. The value of this field indicates the number of bytes of the vendor specific capability as require by the PCI specification. It has the value of 06h for the Function Level Reset capability.

6.1.33 DEVCTRL—Device Control Register (Gigabit LAN—D25:F0)

Address Offset: E4–E5h
Attribute: R/W
Default Value: 0000h
Size: 16 bits

Bit	Description
15:9	Reserved
8	Transactions Pending (TXP) — R/W. 1 = Indicates the controller has issued Non-Posted requests which have not been completed. 0 = Indicates that completions for all Non-Posted requests have been received.
7:1	Reserved
0	**Initiate Function Level Reset** — R/W. This bit is used to initiate an FLT transition. A write of 1 initiates the transition. Since hardware must not respond to any cycles until Function Level Reset completion, the value read by software from this bit is 0.

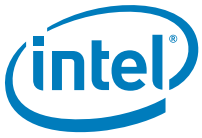
6.2 Gigabit LAN Capabilities and Status Registers (CSR)

The internal CSR registers and memories are accessed as direct memory mapped offsets from the base address register in Section 6.1.10. Software may only access whole DWord at a time.

Note: Register address locations that are not shown in Table 6-1 should be treated as Reserved.

Table 6-2. Gigabit LAN Capabilities and Status Registers Address Map (Gigabit LAN—MBARA)

MBARA + Offset	Mnemonic	Register Name	Default	Attribute
00h–03h	GBECSR_00	Gigabit Ethernet Capabilities and Status Register 00	00100241h	R/W
18h–1Bh	GBECSR_18	Gigabit Ethernet Capabilities and Status Register 18	01501000h	R/W/SN
20h–23h	GBECSR_20	Gigabit Ethernet Capabilities and Status Register 20	1000XXXXh	R/W/V
2Ch–2Fh	GBECSR_2C	Gigabit Ethernet Capabilities and Status Register 2C	00000000h	R/W
F00h–F03h	GBECSR_F00	Gigabit Ethernet Capabilities and Status Register F00	00010008h	R/W/V
F10h–F13h	GBECSR_F10	Gigabit Ethernet Capabilities and Status Register F10	0004000Ch	R/W/SN
5400h–5403h	GBECSR_5400	Gigabit Ethernet Capabilities and Status Register 5400	XXXXXXXXh	R/W
5404h–5407h	GBECSR_5404	Gigabit Ethernet Capabilities and Status Register 5404	XXXXXXXXh	R/W
5800h–5803h	GBECSR_5800	Gigabit Ethernet Capabilities and Status Register 5800	00000008h	R/W/SN
5B54h–5B57h	GBECSR_5B54	Gigabit Ethernet Capabilities and Status Register 5B54	60000040h	RO



6.2.1 GBECSR_00—Gigabit Ethernet Capabilities and Status Register 00

Address Offset: MBARA + 00h
Default Value: 00100241h
Attribute: R/W
Size: 32 bit

Bit	Description
31:25	Reserved
24	PHY Power Down (PHYPDN) — R/W. When cleared (0b), the PHY power down setting is controlled by the internal logic of Intel® Xeon® Processor D-1500 Product Family.
23:0	Reserved

6.2.2 GBECSR_18—Gigabit Ethernet Capabilities and Status Register 18

Address Offset: MBARA + 18h
Default Value: 01501000h
Attribute: R/W/SN
Size: 32 bit

Bit	Description
31:21	Reserved
20	PHY Power Down Enable (PHYPDEN) — R/W/SN. When set, this bit enables the PHY to enter a low-power state when the LAN controller is at the DMoff/D3 or with no WOL.
19:0	Reserved

6.2.3 GBECSR_20—Gigabit Ethernet Capabilities and Status Register 20

Address Offset: MBARA + 20h
Default Value: 1000XXXXh
Attribute: R/W/V
Size: 32 bit

Bit	Description
31	**WAIT** — RO. Set to 1 by the Gigabit Ethernet Controller to indicate that a PCI Express* to SMBus transition is taking place. The ME/Host should not issue new MDIC transactions while this bit is set to 1. This bit is auto cleared by HW after the transition has occurred.
30	**Error** — R/W/V. Set to 1 by the Gigabit Ethernet Controller when it fails to complete an MDI read. Software should make sure this bit is clear before making an MDI read or write command.
29	Reserved
28	Ready Bit (RB) — R/W/V. Set to 1 by the Gigabit Ethernet Controller at the end of the MDI transaction. This bit should be reset to 0 by software at the same time the command is written.
27:26	MDI Type — R/W/V. 01 = MDI Write 10 = MDI Read All other values are reserved.
25:21	LAN Connected Device Address (PHYADD) — R/W/V.
20:16	LAN Connected Device Register Address (PHYREGADD) — R/W/V.
15:0	**DATA** — R/W/V.

6.2.4 GBECSR_2C—Gigabit Ethernet Capabilities and Status Register 2C

Address Offset: MBARA + 2Ch
Attribute: R/W
Default Value: 00000000h
Size: 32 bits

Bit	Description
31	WOL Indication Valid (WIV) — R/W. Set to 1 by BIOS to indicate that the WOL indication setting in bit 30 of this register is valid.
30	WOL Enable Setting by BIOS (WESB) — R/W. 1 = WOL Enabled in BIOS. 0 = WOL Disabled in BIOS.
29:0	Reserved

6.2.5 GBECSR_F00—Gigabit Ethernet Capabilities and Status Register F00

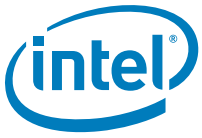
Address Offset: MBARA + F00h
Attribute: R/W/V
Default Value: 00010008h
Size: 32 bits

Bit	Description
31:6	Reserved
5	SW Semaphore FLAG (SWFLAG) — R/W/V. This bit is set by the device driver to gain access permission to shared CSR registers with the firmware and hardware.
4:0	Reserved

6.2.6 GBECSR_F10—Gigabit Ethernet Capabilities and Status Register F10

Address Offset: MBARA + F10h
Attribute: R/W/SN
Default Value: 0004000Ch
Size: 32 bits

Bit	Description
31:7	Reserved
6	Global GbE Disable (GGD)— R/W/SN. Prevents the PHY from auto-negotiating 1000 Mb/s link in all power states.
5:4	Reserved
3	GbE Disable at non D0a — R/W/SN. Prevents the PHY from auto-negotiating 1000 Mb/s link in all power states except D0a. This bit must be set since GbE is not supported in Sx states.
2	LPLU in non D0a (LPLUND) — R/W/SN. Enables the PHY to negotiate for the slowest possible link in all power states except D0a.
1	LPLU in D0a (LPLUD) — R/W/SN. Enables the PHY to negotiate for the slowest possible link in all power states. This bit overrides bit 2.
0	Reserved



6.2.7 GBECSR_5400—Gigabit Ethernet Capabilities and Status Register 5400

Address Offset: MBARA + 5400h Attribute: R/W
Default Value: XXXXXXXXh Size: 32 bits

Bit	Description
31:0	**Receive Address Low (RAL)**— R/W. The lower 32 bits of the 48 bit Ethernet Address.

6.2.8 GBECSR_5404—Gigabit Ethernet Capabilities and Status Register 5404

Address Offset: MBARA + 5404h Attribute: R/W
Default Value: XXXXXXXXh Size: 32 bits

Bit	Description
31	**Address Valid**— R/W.
30:16	Reserved
15:0	**Receive Address High (RAH)**— R/W. The lower 16 bits of the 48 bit Ethernet Address.

6.2.9 GBECSR_5800—Gigabit Ethernet Capabilities and Status Register 5800

Address Offset: MBARA + 5800h Attribute: R/W/SN
Default Value: 00000008h Size: 32 bits

Bit	Description
31:1	Reserved
0	**Advanced Power Management Enable (APME)** — R/W/SN. 1 = APM Wakeup is enabled 0 = APM Wakeup is disabled

6.2.10 GBECSR_5B54—Gigabit Ethernet Capabilities and Status Register 5B54

Address Offset: MBARA + 5B54h Attribute: RO
Default Value: 60000040h Size: 32 bits

Bit	Description
31:16	Reserved
15	**Firmware Valid Bit (FWVAL)** — RO. 1 = Firmware is ready 0 = Firmware is not ready
14:0	Reserved

§

7 LPC Interface Bridge Registers (D31:F0)

The LPC bridge function of Intel® Xeon® Processor D-1500 Product Family resides in PCI D31:F0. This function contains many other functional units, such as DMA and Interrupt controllers, Timers, Power Management, System Management, GPIO, RTC, and LPC Configuration Registers.

Registers and functions associated with other functional units are described in their respective sections.

7.1 PCI Configuration Registers (LPC I/F—D31:F0)

Note: Address locations that are not shown should be treated as Reserved.

Table 7-1. LPC Interface PCI Register Address Map (LPC I/F—D31:F0) (Sheet 1 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
00h–01h	VID	Vendor Identification	8086h	RO
02h–03h	DID	Device Identification	See register description	RO
04h–05h	PCICMD	PCI Command	0007h	R/W, RO
06h–07h	PCISTS	PCI Status	0210h	R/WC, RO
08h	RID	Revision Identification	See register description	R/WO
09h	PI	Programming Interface	00h	RO
0Ah	SCC	Sub Class Code	01h	RO
0Bh	BCC	Base Class Code	06h	RO
0Dh	PLT	Primary Latency Timer	00h	RO
0Eh	HEADTYP	Header Type	80h	RO
2Ch–2Fh	SS	Sub System Identifiers	00000000h	R/WO
40h–43h	PMBASE	ACPI Base Address	00000001h	R/W, RO
44h	ACPI_CNTL	ACPI Control	00h	R/W
48h–4Bh	GPIOBASE	GPIO Base Address	00000001h	R/W, RO
4Ch	GC	GPIO Control	00h	R/W
60h–63h	PIRQ[*n*]_ROUT	PIRQ[A,B,C,D] Routing Control	80808080h	R/W
64h	SIRQ_CNTL	Serial IRQ Control	10h	R/W, RO
68h–6Bh	PIRQ[*n*]_ROUT	PIRQ[E,F,G,H] Routing Control	80808080h	R/W
6Ch–6Dh	LPC_IBDF	IOxAPIC Bus:Device:Function	00F8h	R/W
70h–7Fh	LPC_HnBDF	HPET Configuration	00F8h	R/W
80h	LPC_I/O_DEC	I/O Decode Ranges	0000h	R/W
82h–83h	LPC_EN	LPC I/F Enables	0000h	R/W
84h–87h	GEN1_DEC	LPC I/F Generic Decode Range 1	00000000h	R/W
88h–8Bh	GEN2_DEC	LPC I/F Generic Decode Range 2	00000000h	R/W
8Ch–8Eh	GEN3_DEC	LPC I/F Generic Decode Range 3	00000000h	R/W
90h–93h	GEN4_DEC	LPC I/F Generic Decode Range 4	00000000h	R/W

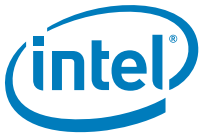


Table 7-1. LPC Interface PCI Register Address Map (LPC I/F—D31:F0) (Sheet 2 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
94h–97h	ULKMC	USB Legacy Keyboard / Mouse Control	00002000h	RO, R/WC, R/W
98h–9Bh	LGMR	LPC I/F Generic Memory Range	00000000h	R/W
A0h–CFh		Power Management (See Section 7.8.1)		
D0h–D3h	BIOS_SEL1	BIOS Select 1	00112233h	R/W, RO
D4h–D5h	BIOS_SEL2	BIOS Select 2	4567h	R/W
D8h–D9h	BIOS_DEC_EN1	BIOS Decode Enable 1	FFCFh	R/W, RO
DCh	BIOS_CNTL	BIOS Control	20h	R/WLO, R/W, RO
E0h–E1h	FDCAP	Feature Detection Capability ID	0009h	RO
E2h	FDLEN	Feature Detection Capability Length	0Ch	RO
E3h	FDVER	Feature Detection Version	10h	RO
E4h–E7h	FVECIDX	Feature Vector Index	00000000h	R/W
E8h–EBh	FVECD	Feature Vector Data	See Description	RO
F0h–F3h	RCBA	Root Complex Base Address	00000000h	R/W

7.1.1 VID—Vendor Identification Register (LPC I/F—D31:F0)

Offset Address: 00h–01h
Default Value: 8086h
Lockable: No
Attribute: RO
Size: 16 bits
Power Well: Core

Bit	Description
15:0	**Vendor ID** — RO. This is a 16-bit value assigned to Intel. Intel VID = 8086h

7.1.2 DID—Device Identification Register (LPC I/F—D31:F0)

Offset Address: 02h–03h
Default Value: See bit description
Lockable: No
Attribute: RO
Size: 16 bits
Power Well: Core

Bit	Description
15:0	**Device ID** — RO. This is a 16-bit value assigned to Intel® Xeon® Processor D-1500 Product Family LPC bridge.

7.1.3 PCICMD—PCI COMMAND Register (LPC I/F—D31:F0)

Offset Address: 04h–05h
Default Value: 0007h
Lockable: No
Attribute: R/W, RO
Size: 16 bits
Power Well: Core

Bit	Description
15:10	Reserved
9	Fast Back to Back Enable (FBE) — RO. Hardwired to 0.
8	**SERR# Enable (SERR_EN)** — R/W. The LPC bridge generates SERR# if this bit is set.
7	Wait Cycle Control (WCC) — RO. Hardwired to 0.

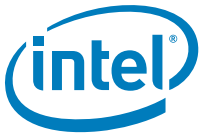
Bit	Description
6	**Parity Error Response Enable (PERE)** — R/W. 0 = No action is taken when detecting a parity error. 1 = Enables Intel® Xeon® Processor D-1500 Product Family LPC bridge to respond to parity errors detected on backbone interface.
5	VGA Palette Snoop (VPS) — RO. Hardwired to 0.
4	Memory Write and Invalidate Enable (MWIE) — RO. Hardwired to 0.
3	Special Cycle Enable (SCE) — RO. Hardwired to 0.
2	Bus Master Enable (BME) — RO. Bus Masters cannot be disabled.
1	Memory Space Enable (MSE) — RO. Memory space cannot be disabled on LPC.
0	I/O Space Enable (IOSE) — RO. I/O space cannot be disabled on LPC.

7.1.4 PCISTS—PCI Status Register (LPC I/F—D31:F0)

Offset Address:	06h–07h	Attribute:	RO, R/WC
Default Value:	0210h	Size:	16 bits
Lockable:	No	Power Well:	Core

Note: For the writable bits, software must write a 1 to clear bits that are set. Writing a 0 to the bit has no effect.

Bit	Description
15	**Detected Parity Error (DPE)** — R/WC. Set when the LPC bridge detects a parity error on the internal backbone. Set even if the PCICMD.PERE bit (D31:F0:04, bit 6) is 0. 0 = All conditions listed below Not met. 1 = Set when all three of the following conditions are met:
14	**Signaled System Error (SSE)**— R/WC. Set when the LPC bridge signals a system error to the internal SERR# logic.
13	**Master Abort Status (RMA)** — R/WC. 0 = Unsupported request status not received. 1 = The bridge received a completion with unsupported request status from the backbone.
12	**Received Target Abort (RTA)** — R/WC. 0 = Completion abort not received. 1 = Completion with completion abort received from the backbone.
11	**Signaled Target Abort (STA)** — R/WC. 0 = Target abort Not generated on the backbone. 1 = LPC bridge generated a completion packet with target abort status on the backbone.
10:9	**DEVSEL# Timing Status (DEV_STS)** — RO. 01 = Medium Timing.
8	**Data Parity Error Detected (DPED)** — R/WC. 0 = All conditions listed below Not met. 1 = Set when all three of the following conditions are met: • LPC bridge receives a completion packet from the backbone from a previous request, • Parity error has been detected (D31:F0:06, bit 15) • PCICMD.PERE bit (D31:F0:04, bit 6) is set.
7	Fast Back to Back Capable (FBC) — RO. Hardwired to 0.
6	Reserved
5	66 MHz Capable (66MHZ_CAP) — RO. Hardwired to 0.
4	**Capabilities List (CLIST)** — RO. Capability list exists on the LPC bridge.
3	**Interrupt Status (IS)** — RO. The LPC bridge does not generate interrupts.
2:0	Reserved



7.1.5 RID—Revision Identification Register (LPC I/F—D31:F0)

Offset Address: 08h Attribute: R/WO
Default Value: See bit description Size: 8 bits

Bit	Description
7:0	**Revision ID (RID)** — R/WO. This field indicates the device specific revision identifier.

7.1.6 PI—Programming Interface Register (LPC I/F—D31:F0)

Offset Address: 09h Attribute: RO
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Programming Interface** — RO.

7.1.7 SCC—Sub Class Code Register (LPC I/F—D31:F0)

Offset Address: 0Ah Attribute: RO
Default Value: 01h Size: 8-bit

Bit	Description
7:0	**Sub Class Code** — RO. 8-bit value that indicates the category of bridge for the LPC bridge. 01h = PCI-to-ISA bridge.

7.1.8 BCC—Base Class Code Register (LPC I/F—D31:F0)

Offset Address: 0Bh Attribute: RO
Default Value: 06h Size: 8-bit

Bit	Description
7:0	**Base Class Code** — RO. 8-bit value that indicates the type of device for the LPC bridge. 06h = Bridge device.

7.1.9 PLT—Primary Latency Timer Register (LPC I/F—D31:F0)

Offset Address: 0Dh Attribute: RO
Default Value: 00h Size: 8-bit

Bit	Description
7:3	Master Latency Count (MLC) — Reserved
2:0	Reserved

7.1.10 HEADTYP—Header Type Register (LPC I/F—D31:F0)

Offset Address: 0Eh Attribute: RO
Default Value: 80h Size: 8-bit

Bit	Description
7	**Multi-Function Device** — RO. This bit is 1 to indicate a multi-function device.
6:0	**Header Type** — RO. This 7-bit field identifies the header layout of the configuration space.

7.1.11 SS—Sub System Identifiers Register (LPC I/F—D31:F0)

Offset Address:	2Ch–2Fh	Attribute:	R/WO
Default Value:	00000000h	Size:	32 bits

This register is initialized to logic 0 by the assertion of PLTRST#. This register can be written only once after PLTRST# de-assertion.

Bit	Description
31:16	**Subsystem ID (SSID)** — R/WO. This is written by BIOS. No hardware action taken on this value.
15:0	**Subsystem Vendor ID (SSVID)** — R/WO. This is written by BIOS. No hardware action taken on this value.

7.1.12 CAPP—Capability List Pointer Register (LPC I/F—D31:F0)

Offset Address:	34h	Attribute:	RO
Default Value:	E0h	Size:	8 bits

Bit	Description
7:0	**Capability Pointer (CP)** — RO. Indicates the offset of the first Capability Item.

7.1.13 PMBASE—ACPI Base Address Register (LPC I/F—D31:F0)

Offset Address:	40h–43h	Attribute:	R/W, RO
Default Value:	00000001h	Size:	32 bits
Lockable:	No	Usage:	ACPI, Legacy
		Power Well:	Core

Sets base address for ACPI I/O registers, GPIO registers and TCO I/O registers. These registers can be mapped anywhere in the 64-K I/O space on 128-byte boundaries.

Bit	Description
31:16	Reserved
15:7	**Base Address** — R/W. This field provides 128 bytes of I/O space for ACPI, GPIO, and TCO logic. This is placed on a 128-byte boundary.
6:1	Reserved
0	Resource Type Indicator (RTE) — RO. Hardwired to 1 to indicate I/O space.

7.1.14 ACPI_CNTL—ACPI Control Register (LPC I/F — D31:F0)

Offset Address:	44h	Attribute:	R/W
Default Value:	00h	Size:	8 bits
Lockable:	No	Usage:	ACPI, Legacy
		Power Well:	Core

Bit	Description
7	**ACPI Enable (ACPI_EN)** — R/W. 0 = Disable. 1 = Decode of the I/O range pointed to by the ACPI base register is enabled, and the ACPI power management function is enabled. The APM power management ranges (B2/B3h) are always enabled and are not affected by this bit.
6:3	Reserved

Bit	Description
2:0	**SCI IRQ Select (SCI_IRQ_SEL)** — R/W. Specifies on which IRQ the SCI will internally appear. If not using the APIC, the SCI must be routed to IRQ9–11, and that interrupt is not sharable with the SERIRQ stream, but is shareable with other PCI interrupts. If using the APIC, the SCI can also be mapped to IRQ20–23, and can be shared with other interrupts. **Bits** — **SCI Map** 000b — IRQ9 001b — IRQ10 010b — IRQ11 011b — Reserved 100b — IRQ20 (Only available if APIC enabled) 101b — IRQ21 (Only available if APIC enabled) 110b — IRQ22 (Only available if APIC enabled) 111b — IRQ23 (Only available if APIC enabled) When the interrupt is mapped to APIC interrupts 9, 10 or 11, the APIC should be programmed for active-high reception. When the interrupt is mapped to APIC interrupts 20 through 23, the APIC should be programmed for active-low reception.

7.1.15 GPIOBASE—GPIO Base Address Register (LPC I/F — D31:F0)

Offset Address: 48h–4Bh Attribute: R/W, RO
Default Value: 00000001h Size: 32 bits

Bit	Description
31:16	Reserved. Always 0.
15:7	**Base Address (BA)** — R/W. Provides the 128 bytes of I/O space for GPIO.
6:1	Reserved. Always 0.
0	RO. Hardwired to 1 to indicate I/O space.

7.1.16 GC—GPIO Control Register (LPC I/F — D31:F0)

Offset Address: 4Ch Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:5	Reserved
4	**GPIO Enable (EN)** — R/W. This bit enables/disables decode of the I/O range pointed to by the GPIO Base Address register (D31:F0:48h) and enables the GPIO function. 0 = Disable. 1 = Enable.
3:1	Reserved

Bit	Description
0	**GPIO Lockdown Enable (GLE)** — R/W. This bit enables lockdown of the following GPIO registers: • Offset 00h: GPIO_USE_SEL • Offset 04h: GP_IO_SEL • Offset 0Ch: GP_LVL • Offset 30h: GPIO_USE_SEL2 • Offset 34h: GP_IO_SEL2 • Offset 38h: GP_LVL2 • Offset 40h: GPIO_USE_SEL3 • Offset 44h: GP_IO_SEL3 • Offset 48h: GP_LVL3 • Offset 60h: GP_RST_SEL 0 = Disable. 1 = Enable. When this bit is written from 1-to-0, an SMI# is generated, if enabled. This ensures that only SMM code can change the above GPIO registers after they are locked down.

7.1.17 PIRQ[n]_ROUT—PIRQ[A,B,C,D] Routing Control Register (LPC I/F—D31:F0)

Offset Address:	PIRQA – 60h, PIRQB – 61h, PIRQC – 62h, PIRQD – 63h	Attribute:	R/W
Default Value:	80h	Size:	8 bits
Lockable:	No	Power Well:	Core

Bit	Description
7	**Interrupt Routing Enable (IRQEN)** — R/W. 0 = The corresponding PIRQ is routed to one of the ISA-compatible interrupts specified in bits[3:0]. 1 = The PIRQ is not routed to the 8259. ***Note:*** BIOS must program this bit to 0 during POST for any of the PIRQs that are being used. The value of this bit may subsequently be changed by the OS when setting up for I/O APIC interrupt delivery mode.
6:4	Reserved
3:0	**IRQ Routing** — R/W. (ISA compatible.) **Value** / **IRQ** / **Value** / **IRQ** 0000b Reserved 1000b Reserved 0001b Reserved 1001b IRQ9 0010b Reserved 1010b IRQ10 0011b IRQ3 1011b IRQ11 0100b IRQ4 1100b IRQ12 0101b IRQ5 1101b Reserved 0110b IRQ6 1110b IRQ14 0111b IRQ7 1111b IRQ15

7.1.18 SIRQ_CNTL—Serial IRQ Control Register (LPC I/F—D31:F0)

Offset Address:	64h	Attribute:	R/W, RO
Default Value:	10h	Size:	8 bits
Lockable:	No	Power Well:	Core

Bit	Description
7	**Serial IRQ Enable (SIRQEN)** — R/W. 0 = The buffer is input only and internally SERIRQ will be a 1. 1 = Serial IRQs will be recognized. The SERIRQ pin will be configured as SERIRQ.
6	**Serial IRQ Mode Select (SIRQMD)** — R/W. 0 = The serial IRQ machine will be in quiet mode. 1 = The serial IRQ machine will be in continuous mode. ***Note:*** For systems using Quiet Mode, this bit should be set to 1 (Continuous Mode) for at least one frame after coming out of reset before switching back to Quiet Mode. Failure to do so will result in Intel® Xeon® Processor D-1500 Product Family not recognizing SERIRQ interrupts.
5:2	**Serial IRQ Frame Size (SIRQSZ)** — RO. Fixed field that indicates the size of the SERIRQ frame as 21 frames.
1:0	**Start Frame Pulse Width (SFPW)** — R/W. This is the number of PCI clocks that the SERIRQ pin will be driven low by the serial IRQ machine to signal a start frame. In continuous mode, Intel® Xeon® Processor D-1500 Product Family will drive the start frame for the number of clocks specified. In quiet mode, Intel® Xeon® Processor D-1500 Product Family will drive the start frame for the number of clocks specified minus one, as the first clock was driven by the peripheral. 00 = 4 clocks 01 = 6 clocks 10 = 8 clocks 11 = Reserved

7.1.19 PIRQ[n]_ROUT—PIRQ[E,F,G,H] Routing Control Register (LPC I/F—D31:F0)

Offset Address:	PIRQE – 68h, PIRQF – 69h, PIRQG – 6Ah, PIRQH – 6Bh	Attribute:	R/W
Default Value:	80h	Size:	8 bits
Lockable:	No	Power Well:	Core

Bit	Description
7	**Interrupt Routing Enable (IRQEN)** — R/W. 0 = The corresponding PIRQ is routed to one of the ISA-compatible interrupts specified in bits[3:0]. 1 = The PIRQ is not routed to the 8259. ***Note:*** BIOS must program this bit to 0 during POST for any of the PIRQs that are being used. The value of this bit may subsequently be changed by the OS when setting up for I/O APIC interrupt delivery mode.
6:4	Reserved
3:0	**IRQ Routing** — R/W. (ISA compatible.)

Value	IRQ	Value	IRQ
0000b	Reserved	1000b	Reserved
0001b	Reserved	1001b	IRQ9
0010b	Reserved	1010b	IRQ10
0011b	IRQ3	1011b	IRQ11
0100b	IRQ4	1100b	IRQ12
0101b	IRQ5	1101b	Reserved
0110b	IRQ6	1110b	IRQ14
0111b	IRQ7	1111b	IRQ15

7.1.20 LPC_IBDF—IOxAPIC Bus:Device:Function (LPC I/F—D31:F0)

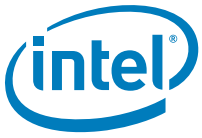
Offset Address: 6Ch–6Dh
Attribute: R/W
Default Value: 00F8h
Size: 16 bits

Bit	Description
15:0	**IOxAPIC Bus:Device:Function (IBDF)**— R/W. this field specifies the bus:device:function that Intel® Xeon® Processor D-1500 Product Family's IOxAPIC will be using for the following: • As the Requester ID when initiating Interrupt Messages to the processor. • As the Completer ID when responding to the reads targeting the IOxAPIC's Memory-Mapped I/O registers. The 16-bit field comprises the following: **Bits** **Description** 15:8 Bus Number 7:3 Device Number 2:0 Function Number This field defaults to Bus 0: Device 31: Function 0 after reset. BIOS can program this field to provide a unique bus:device:function number for the internal IOxAPIC.

7.1.21 LPC_HnBDF—HPET n Bus:Device:Function (LPC I/F—D31:F0)

Address Offset H0BDF 70h–71h
H1BDF 72h–73h
H2BDF 74h–75h
H3BDF 76h–77h
H4BDF 78h–79h
H5BDF 7Ah–7Bh
H6BDF 7Ch–7Dh
H7BDF 7Eh–7Fh
Attribute: R/W
Default Value: 00F8h
Size: 16 bits

Bit	Description
15:0	**HPET n Bus:Device:Function (HnBDF)**— R/W. This field specifies the bus:device:function that Intel® Xeon® Processor D-1500 Product Family's HPET n will be using in the following: • As the Requester ID when initiating Interrupt Messages to the processor • As the Completer ID when responding to the reads targeting the corresponding HPET's Memory-Mapped I/O registers The 16-bit field comprises the following: **Bits** / **Description**: 15:8 Bus Number; 7:3 Device Number; 2:0 Function Number This field is default to Bus 0: Device 31: Function 0 after reset. BIOS shall program this field accordingly if unique bus:device:function number is required for the corresponding HPET.



7.1.22 LPC_I/O_DEC—I/O Decode Ranges Register (LPC I/F—D31:F0)

Offset Address: 80h
Default Value: 0000h
Attribute: R/W
Size: 16 bits

Bit	Description
15:13	Reserved
12	**FDD Decode Range** — R/W. Determines which range to decode for the FDD Port 0 = 3F0h–3F5h, 3F7h (Primary) 1 = 370h–375h, 377h (Secondary)
11:10	Reserved
9:8	**LPT Decode Range** — R/W. This field determines which range to decode for the LPT Port. 00 = 378h–37Fh and 778h–77Fh 01 = 278h–27Fh (port 279h is read only) and 678h–67Fh 10 = 3BCh –3BEh and 7BCh–7BEh 11 = Reserved
7	Reserved
6:4	**COMB Decode Range** — R/W. This field determines which range to decode for the COMB Port. 000 = 3F8h–3FFh (COM1) 001 = 2F8h–2FFh (COM2) 010 = 220h–227h 011 = 228h–22Fh 100 = 238h–23Fh 101 = 2E8h–2EFh (COM4) 110 = 338h–33Fh 111 = 3E8h–3EFh (COM3)
3	Reserved
2:0	**COMA Decode Range** — R/W. This field determines which range to decode for the COMA Port. 000 = 3F8h–3FFh (COM1) 001 = 2F8h–2FFh (COM2) 010 = 220h–227h 011 = 228h–22Fh 100 = 238h–23Fh 101 = 2E8h–2EFh (COM4) 110 = 338h–33Fh 111 = 3E8h–3EFh (COM3)

7.1.23 LPC_EN—LPC I/F Enables Register (LPC I/F—D31:F0)

Offset Address: 82h–83h
Default Value: 0000h
Attribute: R/W
Size: 16 bits
Power Well: Core

Bit	Description
15:14	Reserved
13	**CNF2_LPC_EN** — R/W. Microcontroller Enable #2. 0 = Disable. 1 = Enables the decoding of the I/O locations 4Eh and 4Fh to the LPC interface. This range is used for a microcontroller.
12	**CNF1_LPC_EN** — R/W. Super I/O Enable. 0 = Disable. 1 = Enables the decoding of the I/O locations 2Eh and 2Fh to the LPC interface. This range is used for Super I/O devices.
11	**MC_LPC_EN** — R/W. Microcontroller Enable # 1. 0 = Disable. 1 = Enables the decoding of the I/O locations 62h and 66h to the LPC interface. This range is used for a microcontroller.

Bit	Description
10	**KBC_LPC_EN** — R/W. Keyboard Enable. 0 = Disable. 1 = Enables the decoding of the I/O locations 60h and 64h to the LPC interface. This range is used for a microcontroller.
9	**GAMEH_LPC_EN** — R/W. High Gameport Enable 0 = Disable. 1 = Enables the decoding of the I/O locations 208h to 20Fh to the LPC interface. This range is used for a gameport.
8	**GAMEL_LPC_EN** — R/W. Low Gameport Enable 0 = Disable. 1 = Enables the decoding of the I/O locations 200h to 207h to the LPC interface. This range is used for a gameport.
7:4	Reserved
3	**FDD_LPC_EN** — R/W. Floppy Drive Enable 0 = Disable. 1 = Enables the decoding of the FDD range to the LPC interface. This range is selected in the LPC_FDD/LPT Decode Range Register (D31:F0:80h, bit 12).
2	**LPT_LPC_EN** — R/W. Parallel Port Enable 0 = Disable. 1 = Enables the decoding of the LPTrange to the LPC interface. This range is selected in the LPC_FDD/LPT Decode Range Register (D31:F0:80h, bit 9:8).
1	**COMB_LPC_EN** — R/W. Com Port B Enable 0 = Disable. 1 = Enables the decoding of the COMB range to the LPC interface. This range is selected in the LPC_COM Decode Range Register (D31:F0:80h, bits 6:4).
0	**COMA_LPC_EN** — R/W. Com Port A Enable 0 = Disable. 1 = Enables the decoding of the COMA range to the LPC interface. This range is selected in the LPC_COM Decode Range Register (D31:F0:80h, bits 3:2).

7.1.24 GEN1_DEC—LPC I/F Generic Decode Range 1 Register (LPC I/F—D31:F0)

Offset Address: 84h–87h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits
Power Well: Core

Bit	Description
31:24	Reserved
23:18	**Generic I/O Decode Range Address[7:2] Mask** — R/W. A 1 in any bit position indicates that any value in the corresponding address bit in a received cycle will be treated as a match. The corresponding bit in the Address field, below, is ignored. The mask is only provided for the lower 6 bits of the DWord address, allowing for decoding blocks up to 256 bytes in size.
17:16	Reserved
15:2	**Generic I/O Decode Range 1 Base Address (GEN1_BASE)** — R/W. ***Note:*** Intel® Xeon® Processor D-1500 Product Family does not provide decode down to the word or byte level
1	Reserved
0	**Generic Decode Range 1 Enable (GEN1_EN)** — R/W. 0 = Disable. 1 = Enable the GEN1 I/O range to be forwarded to the LPC I/F

7.1.25 GEN2_DEC—LPC I/F Generic Decode Range 2 Register (LPC I/F—D31:F0)

Offset Address: 88h–8Bh
Default Value: 00000000h
Attribute: R/W
Size: 32 bits
Power Well: Core

Bit	Description
31:24	Reserved
23:18	**Generic I/O Decode Range Address[7:2] Mask —** R/W. A 1 in any bit position indicates that any value in the corresponding address bit in a received cycle will be treated as a match. The corresponding bit in the Address field, below, is ignored. The mask is only provided for the lower 6 bits of the DWord address, allowing for decoding blocks up to 256 bytes in size.
17:16	Reserved
15:2	**Generic I/O Decode Range 2 Base Address (GEN1_BASE)** — R/W. ***Note:*** Intel® Xeon® Processor D-1500 Product Family does not provide decode down to the word or byte level.
1	Reserved
0	**Generic Decode Range 2 Enable (GEN2_EN)** — R/W. 0 = Disable. 1 = Enable the GEN2 I/O range to be forwarded to the LPC I/F

7.1.26 GEN3_DEC—LPC I/F Generic Decode Range 3 Register (LPC I/F—D31:F0)

Offset Address: 8Ch–8Eh
Default Value: 00000000h
Attribute: R/W
Size: 32 bits
Power Well: Core

Bit	Description
31:24	Reserved
23:18	**Generic I/O Decode Range Address[7:2] Mask** — R/W. A 1 in any bit position indicates that any value in the corresponding address bit in a received cycle will be treated as a match. The corresponding bit in the Address field, below, is ignored. The mask is only provided for the lower 6 bits of the DWord address, allowing for decoding blocks up to 256 bytes in size.
17:16	Reserved
15:2	**Generic I/O Decode Range 3 Base Address (GEN3_BASE)** — R/W. ***Note:*** Intel® Xeon® Processor D-1500 Product Family Does not provide decode down to the word or byte level
1	Reserved
0	**Generic Decode Range 3 Enable (GEN3_EN)** — R/W. 0 = Disable. 1 = Enable the GEN3 I/O range to be forwarded to the LPC I/F

7.1.27 GEN4_DEC—LPC I/F Generic Decode Range 4 Register (LPC I/F—D31:F0)

Offset Address: 90h–93h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits
Power Well: Core

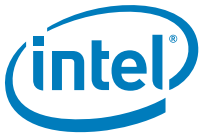
Bit	Description
31:24	Reserved
23:18	**Generic I/O Decode Range Address[7:2] Mask** — R/W. A 1 in any bit position indicates that any value in the corresponding address bit in a received cycle will be treated as a match. The corresponding bit in the Address field, below, is ignored. The mask is only provided for the lower 6 bits of the DWord address, allowing for decoding blocks up to 256 bytes in size.
17:16	Reserved

Bit	Description
15:2	**Generic I/O Decode Range 4 Base Address (GEN4_BASE)** — R/W. ***Note:*** Intel® Xeon® Processor D-1500 Product Family Does not provide decode down to the word or byte level
1	Reserved
0	**Generic Decode Range 4 Enable (GEN4_EN)** — R/W. 0 = Disable. 1 = Enable the GEN4 I/O range to be forwarded to the LPC I/F

7.1.28 ULKMC—USB Legacy Keyboard / Mouse Control Register (LPC I/F—D31:F0)

Offset Address: 94h–97h
Default Value: 00002000h
Attribute: RO, R/WC, R/W
Size: 32 bits
Power Well: Core

Bit	Description
31:16	Reserved
15	**SMI Caused by End of Pass-Through (SMIBYENDPS)** — R/WC. This bit indicates if the event occurred. Even if the corresponding enable bit is not set in bit 7, this bit will still be active. It is up to the SMM code to use the enable bit to determine the exact cause of the SMI#. 0 = Software clears this bit by writing a 1 to the bit location in any of the controllers. 1 = Event Occurred
14:12	Reserved
11	**SMI Caused by Port 64 Write (TRAPBY64W)** — R/WC. This bit indicates if the event occurred. Even if the corresponding enable bit is not set in bit 3, this bit will still be active. It is up to the SMM code to use the enable bit to determine the exact cause of the SMI#. The A20Gate Pass-Through Logic allows specific port 64h writes to complete without setting this bit. 0 = Software clears this bit by writing a 1 to the bit location in any of the controllers. 1 = Event Occurred.
10	**SMI Caused by Port 64 Read (TRAPBY64R)** — R/WC. This bit indicates if the event occurred. Even if the corresponding enable bit is not set in bit 2, this bit will still be active. It is up to the SMM code to use the enable bit to determine the exact cause of the SMI#. 0 = Software clears this bit by writing a 1 to the bit location in any of the controllers. 1 = Event Occurred.
9	**SMI Caused by Port 60 Write (TRAPBY60W)** — R/WC. This bit indicates if the event occurred. Even if the corresponding enable bit is not set in bit 1, this bit will still be active. It is up to the SMM code to use the enable bit to determine the exact cause of the SMI#. The A20Gate Pass-Through Logic allows specific port 64h writes to complete without setting this bit. 0 = Software clears this bit by writing a 1 to the bit location in any of the controllers. 1 = Event Occurred.
8	**SMI Caused by Port 60 Read (TRAPBY60R)** — R/WC. This bit indicates if the event occurred. Even if the corresponding enable bit is not set in the bit 0, this bit will still be active. It is up to the SMM code to use the enable bit to determine the exact cause of the SMI#. 0 = Software clears this bit by writing a 1 to the bit location in any of the controllers. 1 = Event Occurred.
7	**SMI at End of Pass-Through Enable (SMIATENDPS)** — R/W. This bit enables SMI at the end of a pass-through. This can occur if an SMI is generated in the middle of a pass-through, and needs to be serviced later. 0 = Disable 1 = Enable
6	**Pass Through State (PSTATE)** — RO. 0 = If software needs to reset this bit, it should set bit 5 in all of the host controllers to 0. 1 = Indicates that the state machine is in the middle of an A20GATE pass-through sequence.
5	**A20Gate Pass-Through Enable (A20PASSEN)** — R/W. 0 = Disable. 1 = Enable. Allows A20GATE sequence Pass-Through function. A specific cycle sequence involving writes to port 60h and 64h does not result in the setting of the SMI status bits. ***Note:*** A20M# functionality is not supported.



Bit	Description
4	**SMI on USB IRQ Enable (USBSMIEN)** — R/W. 0 = Disable 1 = Enable. USB interrupt will cause an SMI event.
3	**SMI on Port 64 Writes Enable (64WEN)** — R/W. 0 = Disable 1 = Enable. A 1 in bit 11 will cause an SMI event.
2	**SMI on Port 64 Reads Enable (64REN)** — R/W. 0 = Disable 1 = Enable. A 1 in bit 10 will cause an SMI event.
1	**SMI on Port 60 Writes Enable (60WEN)** — R/W. 0 = Disable 1 = Enable. A 1 in bit 9 will cause an SMI event.
0	**SMI on Port 60 Reads Enable (60REN)** — R/W. 0 = Disable 1 = Enable. A 1 in bit 8 will cause an SMI event.

7.1.29 LGMR—LPC I/F Generic Memory Range Register (LPC I/F—D31:F0)

Offset Address: 98h–9Bh
Default Value: 00000000h
Attribute: R/W
Size: 32 bits
Power Well: Core

Bit	Description
31:16	**Memory Address[31:16]** — R/W. This field specifies a 64 KB memory block anywhere in the 4 GB memory space that will be decoded to LPC as standard LPC memory cycle if enabled.
15:1	Reserved
0	**LPC Memory Range Decode Enable** — R/W. When this bit is set to 1, then the range specified in bits 31:16 of this register is enabled for decoding to LPC.

7.1.30 BIOS_SEL1—BIOS Select 1 Register (LPC I/F—D31:F0)

Offset Address: D0h–D3h
Default Value: 00112233h
Attribute: R/W, RO
Size: 32 bits

Bit	Description
31:28	**BIOS_F8_IDSEL** — RO. IDSEL for two 512 KB BIOS memory ranges and one 128 KB memory range. This field is fixed at 0000. The IDSEL programmed in this field addresses the following memory ranges: FFF8 0000h–FFFF FFFFh FFB8 0000h–FFBF FFFFh 000E 0000h–000F FFFFh
27:24	**BIOS_F0_IDSEL** — R/W. IDSEL for two 512 KB BIOS memory ranges. The IDSEL programmed in this field addresses the following memory ranges: FFF0 0000h–FFF7 FFFFh FFB0 0000h–FFB7 FFFFh
23:20	**BIOS_E8_IDSEL** — R/W. IDSEL for two 512 KB BIOS memory ranges. The IDSEL programmed in this field addresses the following memory ranges: FFE8 0000h–FFEF FFFFh FFA8 0000h–FFAF FFFFh
19:16	**BIOS_E0_IDSEL** — R/W. IDSEL for two 512 KB BIOS memory ranges. The IDSEL programmed in this field addresses the following memory ranges: FFE0 0000h–FFE7 FFFFh FFA0 0000h–FFA7 FFFFh

Bit	Description
15:12	**BIOS_D8_IDSEL** — R/W. IDSEL for two 512 KB BIOS memory ranges. The IDSEL programmed in this field addresses the following memory ranges: FFD8 0000h–FFDF FFFFh FF98 0000h–FF9F FFFFh
11:8	**BIOS_D0_IDSEL** — R/W. IDSEL for two 512 KB BIOS memory ranges. The IDSEL programmed in this field addresses the following memory ranges: FFD0 0000h–FFD7 FFFFh FF90 0000h–FF97 FFFFh
7:4	**BIOS_C8_IDSEL** — R/W. IDSEL for two 512 KB BIOS memory ranges. The IDSEL programmed in this field addresses the following memory ranges: FFC8 0000h–FFCF FFFFh FF88 0000h–FF8F FFFFh
3:0	**BIOS_C0_IDSEL** — R/W. IDSEL for two 512 KB BIOS memory ranges. The IDSEL programmed in this field addresses the following memory ranges: FFC0 0000h–FFC7 FFFFh FF80 0000h–FF87 FFFFh

7.1.31 BIOS_SEL2—BIOS Select 2 Register (LPC I/F—D31:F0)

Offset Address: D4h–D5h Attribute: R/W
Default Value: 4567h Size: 16 bits

Bit	Description
15:12	**BIOS_70_IDSEL** — R/W. IDSEL for two, 1MB BIOS memory ranges. The IDSEL programmed in this field addresses the following memory ranges: FF70 0000h–FF7F FFFFh FF30 0000h–FF3F FFFFh
11:8	**BIOS_60_IDSEL** — R/W. IDSEL for two, 1MB BIOS memory ranges. The IDSEL programmed in this field addresses the following memory ranges: FF60 0000h–FF6F FFFFh FF20 0000h–FF2F FFFFh
7:4	**BIOS_50_IDSEL** — R/W. IDSEL for two, 1MB BIOS memory ranges. The IDSEL programmed in this field addresses the following memory ranges: FF50 0000h–FF5F FFFFh FF10 0000h–FF1F FFFFh
3:0	**BIOS_40_IDSEL** — R/W. IDSEL for two, 1MB BIOS memory ranges. The IDSEL programmed in this field addresses the following memory ranges: FF40 0000h–FF4F FFFFh FF00 0000h–FF0F FFFFh

7.1.32 BIOS_DEC_EN1—BIOS Decode Enable Register (LPC I/F—D31:F0)

Offset Address: D8h–D9h Attribute: R/W, RO
Default Value: FFCFh Size: 16 bits

Bit	Description
15	**BIOS_F8_EN** — RO. This bit enables decoding two 512 KB BIOS memory ranges, and one 128-KB memory range. 0 = Disable 1 = Enable the following ranges for the BIOS FFF80000h–FFFFFFFFh FFB80000h–FFBFFFFFh
14	**BIOS_F0_EN** — R/W. This bit enables decoding two 512 KB BIOS memory ranges. 0 = Disable. 1 = Enable the following ranges for the BIOS: FFF00000h–FFF7FFFFh FFB00000h–FFB7FFFFh

Bit	Description
13	**BIOS_E8_EN** — R/W. This bit enables decoding two 512 KB BIOS memory ranges. 0 = Disable. 1 = Enable the following ranges for the BIOS: FFE80000h–FFEFFFFh FFA80000h–FFAFFFFFh
12	**BIOS_E0_EN** — R/W. This bit enables decoding two 512 KB BIOS memory ranges. 0 = Disable. 1 = Enable the following ranges for the BIOS: FFE00000h–FFE7FFFFh FFA00000h–FFA7FFFFh
11	**BIOS_D8_EN** — R/W. This bit enables decoding two 512 KB BIOS memory ranges. 0 = Disable. 1 = Enable the following ranges for the BIOS FFD80000h–FFDFFFFFh FF980000h–FF9FFFFFh
10	**BIOS_D0_EN** — R/W. This bit enables decoding two 512 KB BIOS memory ranges. 0 = Disable. 1 = Enable the following ranges for the BIOS FFD00000h–FFD7FFFFh FF900000h–FF97FFFFh
9	**BIOS_C8_EN** — R/W. This bit enables decoding two 512 KB BIOS memory ranges. 0 = Disable. 1 = Enable the following ranges for the BIOS FFC80000h–FFCFFFFFh FF880000h–FF8FFFFFh
8	**BIOS_C0_EN** — R/W. This bit enables decoding two 512 KB BIOS memory ranges. 0 = Disable. 1 = Enable the following ranges for the BIOS FFC00000h–FFC7FFFFh FF800000h–FF87FFFFh
7	**BIOS_Legacy_F_EN** — R/W. This enables the decoding of the legacy 64 KB range at F0000h–FFFFFh. 0 = Disable. 1 = Enable the following legacy ranges for the BIOS F0000h–FFFFFh ***Note:*** The decode for the BIOS legacy F segment is enabled only by this bit and is not affected by the GEN_PMCON_1.iA64_EN bit.
6	**BIOS_Legacy_E_EN** — R/W. This enables the decoding of the legacy 64 KB range at E0000h–EFFFFh. 0 = Disable. 1 = Enable the following legacy ranges for the BIOS E0000h–EFFFFh ***Note:*** The decode for the BIOS legacy E segment is enabled only by this bit and is not affected by the GEN_PMCON_1.iA64_EN bit.
5:4	Reserved
3	**BIOS_70_EN** — R/W. Enables decoding two 1MB BIOS memory ranges. 0 = Disable. 1 = Enable the following ranges for the BIOS FF70 0000h–FF7F FFFFh FF30 0000h–FF3F FFFFh
2	**BIOS_60_EN** — R/W. Enables decoding two 1MB BIOS memory ranges. 0 = Disable. 1 = Enable the following ranges for the BIOS FF60 0000h–FF6F FFFFh FF20 0000h–FF2F FFFFh
1	**BIOS_50_EN** — R/W. Enables decoding two 1MB BIOS memory ranges. 0 = Disable. 1 = Enable the following ranges for the BIOS FF50 0000h–FF5F FFFFh FF10 0000h–FF1F FFFFh

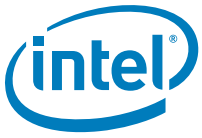
Bit	Description
0	**BIOS_40_EN** — R/W. Enables decoding two 1MB BIOS memory ranges. 0 = Disable. 1 = Enable the following ranges for the BIOS FF40 0000h–FF4F FFFFh FF00 0000h–FF0F FFFFh

Note: This register effects the BIOS decode regardless of whether the BIOS is resident on LPC or SPI. The concept of Feature Space does not apply to SPI-based flash. Intel® Xeon® Processor D-1500 Product Family simply decodes these ranges as memory accesses when enabled for the SPI flash interface.

7.1.33 BIOS_CNTL—BIOS Control Register (LPC I/F—D31:F0)

Offset Address:	DCh	Attribute:	R/WLO, R/W, RO
Default Value:	20h	Size:	8 bits
Lockable:	No	Power Well:	Core

Bit	Description
7:6	Reserved
5	**SMM BIOS Write Protect Disable (SMM_BWP)**— R/WL. This bit set defines when the BIOS region can be written by the host. 0 = BIOS region SMM protection is disabled. The BIOS Region is writable regardless if processors are in SMM or not. (Set this field to 0 for legacy behavior). 1 = BIOS region SMM protection is enabled. The BIOS Region is not writable unless all processors are in SMM and BIOS Write Enable (BIOSWE) is set to '1'.
4	**Top Swap Status (TSS)** — RO. This bit provides a read-only path to view the state of the Top Swap bit that is at offset 3414h, bit 0.
3:2	**SPI Read Configuration (SRC)** — R/W. This 2-bit field controls two policies related to BIOS reads on the SPI interface: Bit 3 – Prefetch Enable Bit 2 – Cache Disable Settings are summarized below: **Bits 3:2** — **Description** 00b — **No prefetching, but caching enabled.** 64B demand reads load the read buffer cache with "valid" data, allowing repeated code fetches to the same line to complete quickly. 01b — **No prefetching and no caching.** One-to-one correspondence of host BIOS reads to SPI cycles. This value can be used to invalidate the cache. 10b — **Prefetching and Caching enabled.** This mode is used for long sequences of short reads to consecutive addresses (that is, shadowing). 11b — **Reserved. This is an invalid configuration**, caching must be enabled when prefetching is enabled.
1	**BIOS Lock Enable (BLE)** — R/WLO. 0 = Transition of BIOSWE from '0' to '1' will not cause an SMI to be asserted. 1 = Enables setting the BIOSWE bit to cause SMIs and locks SMM_BWP. Once set, this bit can only be cleared by a PLTRST#.
0	**BIOS Write Enable (BIOSWE)** — R/W. 0 = Only read cycles result in Firmware Hub or SPI I/F cycles. 1 = Access to the BIOS space is enabled for both read and write cycles. When this bit is written from a 0 to a 1 and BIOS Lock Enable (BLE) is also set, an SMI# is generated. This ensures that only SMI code can update BIOS.



7.1.34 FDCAP—Feature Detection Capability ID Register (LPC I/F—D31:F0)

Offset Address: E0h–E1h
Default Value: 0009h
Attribute: RO
Size: 16 bits
Power Well: Core

Bit	Description
15:8	**Next Item Pointer (NEXT)** — RO. Configuration offset of the next Capability Item. 00h indicates the last item in the Capability List.
7:0	**Capability ID** — RO. Indicates a Vendor Specific Capability

7.1.35 FDLEN—Feature Detection Capability Length Register (LPC I/F—D31:F0)

Offset Address: E2h
Default Value: 0Ch
Attribute: RO
Size: 8 bits
Power Well: Core

Bit	Description
7:0	**Capability Length** — RO. Indicates the length of this Vendor Specific capability, as required by PCI Specification.

7.1.36 FDVER—Feature Detection Version Register (LPC I/F—D31:F0)

Offset Address: E3h
Default Value: 10h
Attribute: RO
Size: 8 bits
Power Well: Core

Bit	Description
7:4	**Vendor-Specific Capability ID** — RO. A value of 1h in this 4-bit field identifies this Capability as Feature Detection Type. This field allows software to differentiate the Feature Detection Capability from other Vendor-Specific capabilities
3:0	**Capability Version** — RO. This field indicates the version of the Feature Detection capability

7.1.37 FVECIDX—Feature Vector Index Register (LPC I/F—D31:F0)

Offset Address: E4h–E7h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits
Power Well: Core

Bit	Description
31:6	Reserved
5:2	**Index (IDX)** — R/W. 4-bit index pointer into the 64-byte Feature Vector space. Data is read from the FVECD register. This points to a DWord register.
1:0	Reserved

7.1.38 FVECD—Feature Vector Data Register (LPC I/F—D31:F0)

Offset Address: E8h–EBh
Default Value: See Description
Attribute: RO
Size: 32 bits
Power Well: Core

Bit	Description
31:0	**Data (DATA)** — RO. 32-bit data value that is read from the Feature Vector offset pointed to by FVECIDX.

7.1.39 Feature Vector Space

7.1.39.1 FVEC0—Feature Vector Register 0

FVECIDX.IDX: 0000b
Default Value: See Description
Attribute: RO
Size: 32 bits
Power Well: Core

Bit	Description
31:12	Reserved
11:10	USB Port Count Capability — RO 00 = 14 ports 01 = 12 ports 10 = 10 ports 11 = Reserved
9:8	Reserved
7	RAID Capability Bit 1 — RO See bit 5 Description.
6	SATA Ports 2 and 3 — RO 0 = Capable 1 = Disabled
5:4	Reserved
3	SATA Port 1 6 Gb/s Capability— RO 0 = Capable 1 = Disabled
2	SATA Port 0 6 Gb/s Capability— RO 0 = Capable 1 = Disabled
1	PCI Interface Capability — RO 0 = Capable 1 = Disabled
0	Reserved

7.1.39.2 FVEC1—Feature Vector Register 1

FVECIDX.IDX: 0001b
Default Value: See Description
Attribute: RO
Size: 32 bits
Power Well: Core

Bit	Description
31:23	Reserved
22	USB Redirect (USBr) Capability— RO 0 = Capable 1 = Disabled
21:0	Reserved

7.1.39.3 FVEC2—Feature Vector Register 2

FVECIDX.IDX: 0010b
Default Value: See Description
Attribute: RO
Size: 32 bits
Power Well: Core

Bit	Description
31:22	Reserved
21	PCI Express* Ports 7 and 8— RO 0 = Capable 1 = Disabled
20:18	Reserved
17	Intel® Xeon® Processor D-1500 Product Family Integrated Graphics Support Capability — RO 0 = Capable 1 = Disabled
16:0	Reserved

7.1.39.4 FVEC3—Feature Vector Register 3

FVECIDX.IDX: 0011b
Default Value: See Description
Attribute: RO
Size: 32 bits
Power Well: Core

Bit	Description
31:14	Reserved
13	Data Center Manageability Interface (DCMI) Capability — RO 0 = Capable 1 = Disabled
12	Node Manager Capability — RO 0 = Capable 1 = Disabled
11:0	Reserved

7.1.40 RCBA—Root Complex Base Address Register (LPC I/F—D31:F0)

Offset Address: F0–F3h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits

Bit	Description
31:14	**Base Address (BA)** — R/W. Base Address for the root complex register block decode range. This address is aligned on a 16 KB boundary.
13:1	Reserved
0	**Enable (EN)** — R/W. When set, this bit enables the range specified in BA to be claimed as the Root Complex Register Block.

7.2 DMA I/O Registers

Table 7-2. DMA Registers (Sheet 1 of 2)

Port	Alias	Register Name	Default	Type
00h	10h	Channel 0 DMA Base and Current Address	Undefined	R/W
01h	11h	Channel 0 DMA Base and Current Count	Undefined	R/W
02h	12h	Channel 1 DMA Base and Current Address	Undefined	R/W
03h	13h	Channel 1 DMA Base and Current Count	Undefined	R/W

Table 7-2. DMA Registers (Sheet 2 of 2)

Port	Alias	Register Name	Default	Type
04h	14h	Channel 2 DMA Base and Current Address	Undefined	R/W
05h	15h	Channel 2 DMA Base and Current Count	Undefined	R/W
06h	16h	Channel 3 DMA Base and Current Address	Undefined	R/W
07h	17h	Channel 3 DMA Base and Current Count	Undefined	R/W
08h	18h	Channel 0–3 DMA Command	Undefined	WO
		Channel 0–3 DMA Status	Undefined	RO
0Ah	1Ah	Channel 0–3 DMA Write Single Mask	000001XXb	WO
0Bh	1Bh	Channel 0–3 DMA Channel Mode	000000XXb	WO
0Ch	1Ch	Channel 0–3 DMA Clear Byte Pointer	Undefined	WO
0Dh	1Dh	Channel 0–3 DMA Master Clear	Undefined	WO
0Eh	1Eh	Channel 0–3 DMA Clear Mask	Undefined	WO
0Fh	1Fh	Channel 0–3 DMA Write All Mask	0Fh	R/W
80h	90h	Reserved Page	Undefined	R/W
81h	91h	Channel 2 DMA Memory Low Page	Undefined	R/W
82h	—	Channel 3 DMA Memory Low Page	Undefined	R/W
83h	93h	Channel 1 DMA Memory Low Page	Undefined	R/W
84h–86h	94h–96h	Reserved Pages	Undefined	R/W
87h	97h	Channel 0 DMA Memory Low Page	Undefined	R/W
88h	98h	Reserved Page	Undefined	R/W
89h	99h	Channel 6 DMA Memory Low Page	Undefined	R/W
8Ah	9Ah	Channel 7 DMA Memory Low Page	Undefined	R/W
8Bh	9Bh	Channel 5 DMA Memory Low Page	Undefined	R/W
8Ch–8Eh	9Ch–9Eh	Reserved Page	Undefined	R/W
8Fh	9Fh	Refresh Low Page	Undefined	R/W
C0h	C1h	Channel 4 DMA Base and Current Address	Undefined	R/W
C2h	C3h	Channel 4 DMA Base and Current Count	Undefined	R/W
C4h	C5h	Channel 5 DMA Base and Current Address	Undefined	R/W
C6h	C7h	Channel 5 DMA Base and Current Count	Undefined	R/W
C8h	C9h	Channel 6 DMA Base and Current Address	Undefined	R/W
CAh	CBh	Channel 6 DMA Base and Current Count	Undefined	R/W
CCh	CDh	Channel 7 DMA Base and Current Address	Undefined	R/W
CEh	CFh	Channel 7 DMA Base and Current Count	Undefined	R/W
D0h	D1h	Channel 4–7 DMA Command	Undefined	WO
		Channel 4–7 DMA Status	Undefined	RO
D4h	D5h	Channel 4–7 DMA Write Single Mask	000001XXb	WO
D6h	D7h	Channel 4–7 DMA Channel Mode	000000XXb	WO
D8h	D9h	Channel 4–7 DMA Clear Byte Pointer	Undefined	WO
DAh	dBh	Channel 4–7 DMA Master Clear	Undefined	WO
DCh	DDh	Channel 4–7 DMA Clear Mask	Undefined	WO
DEh	DFh	Channel 4–7 DMA Write All Mask	0Fh	R/W

7.2.1 DMABASE_CA—DMA Base and Current Address Registers

I/O Address:	Ch. #0 = 00h; Ch. #1 = 02h Ch. #2 = 04h; Ch. #3 = 06h Ch. #5 = C4h Ch. #6 = C8h Ch. #7 = CCh;	Attribute: Size:	R/W 16 bits (per channel), but accessed in two 8 bits quantities
Default Value:	Undefined		
Lockable:	No	Power Well:	Core

Bit	Description
15:0	**Base and Current Address** — R/W. This register determines the address for the transfers to be performed. The address specified points to two separate registers. On writes, the value is stored in the *Base Address* register and copied to the *Current Address* register. On reads, the value is returned from the *Current Address* register. The address increments/decrements in the Current Address register after each transfer, depending on the mode of the transfer. If the channel is in auto-initialize mode, the Current Address register will be reloaded from the Base Address register after a terminal count is generated. For transfers to/from a 16-bit slave (channels 5–7), the address is shifted left one bit location. Bit 15 will be shifted into Bit 16. The register is accessed in 8 bit quantities. The byte is pointed to by the current byte pointer flip/flop. Before accessing an address register, the byte pointer flip/flop should be cleared to ensure that the low byte is accessed first.

7.2.2 DMABASE_CC—DMA Base and Current Count Registers

I/O Address:	Ch. #0 = 01h; Ch. #1 = 03h Ch. #2 = 05h; Ch. #3 = 07h Ch. #5 = C6h; Ch. #6 = CAh Ch. #7 = CEh;	Attribute: Size:	R/W 16 bits (per channel), but accessed in two 8 bits quantities
Default Value:	Undefined		
Lockable:	No	Power Well:	Core

Bit	Description
15:0	**Base and Current Count** — R/W. This register determines the number of transfers to be performed. The address specified points to two separate registers. On writes, the value is stored in the *Base Count* register and copied to the *Current Count* register. On reads, the value is returned from the *Current Count* register. The actual number of transfers is one more than the number programmed in the Base Count Register (that is, programming a count of 4h results in 5 transfers). The count is decrements in the Current Count register after each transfer. When the value in the register rolls from 0 to FFFFh, a terminal count is generated. If the channel is in auto-initialize mode, the Current Count register will be reloaded from the Base Count register after a terminal count is generated. For transfers to/from an 8-bit slave (channels 0–3), the count register indicates the number of bytes to be transferred. For transfers to/from a 16-bit slave (channels 5–7), the count register indicates the number of words to be transferred. The register is accessed in 8 bit quantities. The byte is pointed to by the current byte pointer flip/flop. Before accessing a count register, the byte pointer flip/flop should be cleared to ensure that the low byte is accessed first.

7.2.3 DMAMEM_LP—DMA Memory Low Page Registers

I/O Address: Ch. #0 = 87h; Ch. #1 = 83h
Ch. #2 = 81h; Ch. #3 = 82h
Ch. #5 = 8Bh; Ch. #6 = 89h
Ch. #7 = 8Ah;
Attribute: R/W
Default Value: Undefined
Size: 8 bits
Lockable: No
Power Well: Core

Bit	Description
7:0	**DMA Low Page** (ISA Address bits [23:16]) — R/W. This register works in conjunction with the DMA controller's Current Address Register to define the complete 24-bit address for the DMA channel. This register remains static throughout the DMA transfer. Bit 16 of this register is ignored when in 16 bit I/O count by words mode as it is replaced by the bit 15 shifted out from the current address register.

7.2.4 DMACMD—DMA Command Register

I/O Address: Ch. #0–3 = 08h;
Ch. #4–7 = D0h
Attribute: WO
Default Value: Undefined
Size: 8 bits
Lockable: No
Power Well: Core

Bit	Description
7:5	Reserved. Must be 0.
4	**DMA Group Arbitration Priority** — WO. Each channel group is individually assigned either fixed or rotating arbitration priority. At part reset, each group is initialized in fixed priority. 0 = Fixed priority to the channel group 1 = Rotating priority to the group.
3	Reserved. Must be 0.
2	**DMA Channel Group Enable** — WO. Both channel groups are enabled following part reset. 0 = Enable the DMA channel group. 1 = Disable. Disabling channel group 4–7 also disables channel group 0–3, which is cascaded through channel 4.
1:0	Reserved. Must be 0.

7.2.5 DMASTA—DMA Status Register

I/O Address: Ch. #0–3 = 08h;
Ch. #4–7 = D0h
Attribute: RO
Default Value: Undefined
Size: 8 bits
Lockable: No
Power Well: Core

Bit	Description
7:4	**Channel Request Status** — RO. When a valid DMA request is pending for a channel, the corresponding bit is set to 1. When a DMA request is not pending for a particular channel, the corresponding bit is set to 0. The source of the DREQ may be hardware or a software request. Channel 4 is the cascade channel; thus, the request status of channel 4 is a logical OR of the request status for channels 0 through 3. 4 = Channel 0 5 = Channel 1 (5) 6 = Channel 2 (6) 7 = Channel 3 (7)
3:0	**Channel Terminal Count Status** — RO. When a channel reaches terminal count (TC), its status bit is set to 1. If TC has not been reached, the status bit is cleared to 0. Channel 4 is programmed for cascade; thus, the TC bit response for channel 4 is irrelevant: 0 = Channel 0 1 = Channel 1 (5) 2 = Channel 2 (6) 3 = Channel 3 (7)

7.2.6 DMA_WRSMSK—DMA Write Single Mask Register

I/O Address: Ch. #0–3 = 0Ah; Ch. #4–7 = D4h
Attribute: WO
Default Value: 0000 01xx
Size: 8 bits
Lockable: No
Power Well: Core

Bit	Description
7:3	Reserved. Must be 0.
2	**Channel Mask Select** — WO. 0 = Enable DREQ for the selected channel. The channel is selected through bits [1:0]. Therefore, only one channel can be masked / unmasked at a time. 1 = Disable DREQ for the selected channel.
1:0	**DMA Channel Select** — WO. These bits select the DMA Channel Mode Register to program. 00 = Channel 0 (4) 01 = Channel 1 (5) 10 = Channel 2 (6) 11 = Channel 3 (7)

7.2.7 DMACH_MODE—DMA Channel Mode Register

I/O Address: Ch. #0–3 = 0Bh; Ch. #4–7 = D6h
Attribute: WO
Default Value: 0000 00xx
Size: 8 bits
Lockable: No
Power Well: Core

Bit	Description
7:6	**DMA Transfer Mode** — WO. Each DMA channel can be programmed in one of four different modes: 00 = Demand mode 01 = Single mode 10 = Reserved 11 = Cascade mode
5	**Address Increment/Decrement Select** — WO. This bit controls address increment/decrement during DMA transfers. 0 = Address increment. (default after part reset or Master Clear) 1 = Address decrement.
4	**Autoinitialize Enable** — WO. 0 = Autoinitialize feature is disabled and DMA transfers terminate on a terminal count. A part reset or Master Clear disables autoinitialization. 1 = DMA restores the Base Address and Count registers to the current registers following a terminal count (TC).
3:2	**DMA Transfer Type** — WO. These bits represent the direction of the DMA transfer. When the channel is programmed for cascade mode, (bits [7:6] = 11) the transfer type is irrelevant. 00 = Verify – No I/O or memory strobes generated 01 = Write – Data transferred from the I/O devices to memory 10 = Read – Data transferred from memory to the I/O device 11 = Invalid
1:0	**DMA Channel Select** — WO. These bits select the DMA Channel Mode Register that will be written by bits [7:2]. 00 = Channel 0 (4) 01 = Channel 1 (5) 10 = Channel 2 (6) 11 = Channel 3 (7)

7.2.8 DMA Clear Byte Pointer Register

I/O Address: Ch. #0–3 = 0Ch; Ch. #4–7 = D8h
Attribute: WO
Default Value: xxxx xxxx
Size: 8 bits
Lockable: No
Power Well: Core

Bit	Description
7:0	**Clear Byte Pointer** — WO. No specific pattern. Command enabled with a write to the I/O port address. Writing to this register initializes the byte pointer flip/flop to a known state. It clears the internal latch used to address the upper or lower byte of the 16-bit Address and Word Count Registers. The latch is also cleared by part reset and by the Master Clear command. This command precedes the first access to a 16-bit DMA controller register. The first access to a 16-bit register will then access the significant byte, and the second access automatically accesses the most significant byte.

7.2.9 DMA Master Clear Register

I/O Address: Ch. #0–3 = 0Dh; Ch. #4–7 = DAh
Attribute: WO
Default Value: xxxx xxxx
Size: 8 bits

Bit	Description
7:0	**Master Clear** — WO. No specific pattern. Enabled with a write to the port. This has the same effect as the hardware Reset. The Command, Status, Request, and Byte Pointer flip/flop registers are cleared and the Mask Register is set.

7.2.10 DMA_CLMSK—DMA Clear Mask Register

I/O Address: Ch. #0–3 = 0Eh; Ch. #4–7 = DCh
Attribute: WO
Default Value: xxxx xxxx
Size: 8 bits
Lockable: No
Power Well: Core

Bit	Description
7:0	**Clear Mask Register** — WO. No specific pattern. Command enabled with a write to the port.

7.2.11 DMA_WRMSK—DMA Write All Mask Register

I/O Address: Ch. #0–3 = 0Fh; Ch. #4–7 = DEh
Attribute: R/W
Default Value: 0000 1111
Size: 8 bits
Lockable: No
Power Well: Core

Bit	Description
7:4	Reserved. Must be 0.

Bit	Description
3:0	**Channel Mask Bits** — R/W. This register permits all four channels to be simultaneously enabled/disabled instead of enabling/disabling each channel individually, as is the case with the Mask Register – Write Single Mask Bit. In addition, this register has a read path to allow the status of the channel mask bits to be read. A channel's mask bit is automatically set to 1 when the Current Byte/Word Count Register reaches terminal count (unless the channel is in auto-initialization mode). Setting the bit(s) to a 1 disables the corresponding DREQ(s). Setting the bit(s) to a 0 enables the corresponding DREQ(s). Bits [3:0] are set to 1 upon part reset or Master Clear. When read, bits [3:0] indicate the DMA channel [3:0] ([7:4]) mask status. Bit 0 = Channel 0 (4)1 = Masked, 0 = Not Masked Bit 1 = Channel 1 (5)1 = Masked, 0 = Not Masked Bit 2 = Channel 2 (6)1 = Masked, 0 = Not Masked Bit 3 = Channel 3 (7)1 = Masked, 0 = Not Masked ***Note:*** Disabling channel 4 also disables channels 0–3 due to the cascade of channels 0–3 through channel 4.

7.3 Timer I/O Registers

Port	Aliases	Register Name	Default Value	Type
40h	50h	Counter 0 Interval Time Status Byte Format	0XXXXXXXb	RO
		Counter 0 Counter Access Port	Undefined	R/W
41h	51h	Counter 1 Interval Time Status Byte Format	0XXXXXXXb	RO
		Counter 1 Counter Access Port	Undefined	R/W
42h	52h	Counter 2 Interval Time Status Byte Format	0XXXXXXXb	RO
		Counter 2 Counter Access Port	Undefined	R/W
43h	53h	Timer Control Word	Undefined	WO
		Timer Control Word Register	XXXXXXX0b	WO
		Counter Latch Command	X0h	WO

7.3.1 TCW—Timer Control Word Register

I/O Address: 43h Attribute: WO
Default Value: All bits undefined Size: 8 bits

This register is programmed prior to any counter being accessed to specify counter modes. Following part reset, the control words for each register are undefined and each counter output is 0. Each timer must be programmed to bring it into a known state.

Bit	Description
7:6	**Counter Select** — WO. The Counter Selection bits select the counter the control word acts upon as shown below. The Read Back Command is selected when bits[7:6] are both 1. 00 = Counter 0 select 01 = Counter 1 select 10 = Counter 2 select 11 = Read Back Command
5:4	**Read/Write Select** — WO. These bits are the read/write control bits. The actual counter programming is done through the counter port (40h for counter 0, 41h for counter 1, and 42h for counter 2). 00 = Counter Latch Command 01 = Read/Write Least Significant Byte (LSB) 10 = Read/Write Most Significant Byte (MSB) 11 = Read/Write LSB then MSB

Bit	Description
3:1	**Counter Mode Selection** — WO. These bits select one of six possible modes of operation for the selected counter. **Bit Value** — **Mode** 000b — Mode 0 Out signal on end of count (=0) 001b — Mode 1 Hardware retriggerable one-shot x10b — Mode 2 Rate generator (divide by n counter) x11b — Mode 3 Square wave output 100b — Mode 4 Software triggered strobe 101b — Mode 5 Hardware triggered strobe
0	Binary/BCD Countdown Select — WO. 0 = Binary countdown is used. The largest possible binary count is 2^{16} 1 = Binary coded decimal (BCD) count is used. The largest possible BCD count is 10^4

There are two special commands that can be issued to the counters through this register, the Read Back Command and the Counter Latch Command. When these commands are chosen, several bits within this register are redefined. These register formats are described as follows:

RdBK_CMD—Read Back Command

The Read Back Command is used to determine the count value, programmed mode, and current states of the OUT pin and Null count flag of the selected counter or counters. Status and/or count may be latched in any or all of the counters by selecting the counter during the register write. The count and status remain latched until read, and further latch commands are ignored until the count is read. Both count and status of the selected counters may be latched simultaneously by setting both bit 5 and bit 4 to 0. If both are latched, the first read operation from that counter returns the latched status. The next one or two reads, depending on whether the counter is programmed for one or two byte counts, returns the latched count. Subsequent reads return an unlatched count.

Bit	Description
7:6	**Read Back Command.** Must be 11 to select the Read Back Command
5	**Latch Count of Selected Counters**. 0 = Current count value of the selected counters will be latched 1 = Current count will not be latched
4	**Latch Status of Selected Counters**. 0 = Status of the selected counters will be latched 1 = Status will not be latched
3	**Counter 2 Select**. 1 = Counter 2 count and/or status will be latched
2	**Counter 1 Select**. 1 = Counter 1 count and/or status will be latched
1	**Counter 0 Select**. 1 = Counter 0 count and/or status will be latched.
0	Reserved. Must be 0.

LTCH_CMD—Counter Latch Command

The Counter Latch Command latches the current count value. This command is used to insure that the count read from the counter is accurate. The count value is then read from each counter's count register through the Counter Ports Access Ports Register (40h for counter 0, 41h for counter 1, and 42h for counter 2). The count must be read according to the programmed format; that is, if the counter is programmed for two byte counts, two bytes must be read. The two bytes do not have to be read one right after the other (read, write, or programming operations for other counters may be inserted between the reads). If a counter is latched once and then latched again before the count is read, the second Counter Latch Command is ignored.

Bit	Description
7:6	**Counter Selection.** These bits select the counter for latching. If "11" is written, then the write is interpreted as a read back command. 00 = Counter 0 01 = Counter 1 10 = Counter 2
5:4	**Counter Latch Command**. 00 = Selects the Counter Latch Command.
3:0	Reserved. Must be 0.

7.3.2 SBYTE_FMT—Interval Timer Status Byte Format Register

I/O Address: Counter 0 = 40h, Counter 1 = 41h, Counter 2 = 42h
Attribute: RO
Size: 8 bits per counter
Default Value: Bits[6:0] undefined, Bit 7=0

Each counter's status byte can be read following a Read Back Command. If latch status is chosen (bit 4=0, Read Back Command) as a read back option for a given counter, the next read from the counter's Counter Access Ports Register (40h for counter 0, 41h for counter 1, and 42h for counter 2) returns the status byte. The status byte returns the following:

Bit	Description
7	**Counter OUT Pin State** — RO. 0 = OUT pin of the counter is also a 0 1 = OUT pin of the counter is also a 1
6	**Count Register Status** — RO. This bit indicates when the last count written to the Count Register (CR) has been loaded into the counting element (CE). The exact time this happens depends on the counter mode, but until the count is loaded into the counting element (CE), the count value will be incorrect. 0 = Count has been transferred from CR to CE and is available for reading. 1 = Null Count. Count has not been transferred from CR to CE and is not yet available for reading.
5:4	**Read/Write Selection Status** — RO. These reflect the read/write selection made through bits[5:4] of the control register. The binary codes returned during the status read match the codes used to program the counter read/write selection. 00 = Counter Latch Command 01 = Read/Write Least Significant Byte (LSB) 10 = Read/Write Most Significant Byte (MSB) 11 = Read/Write LSB then MSB

Bit	Description
3:1	**Mode Selection Status** — RO. These bits return the counter mode programming. The binary code returned matches the code used to program the counter mode, as listed under the bit function above. 000 = Mode 0 — Out signal on end of count (=0) 001 = Mode 1 — Hardware retriggerable one-shot x10 = Mode 2 — Rate generator (divide by n counter) x11 = Mode 3 — Square wave output 100 = Mode 4 — Software triggered strobe 101 = Mode 5 — Hardware triggered strobe
0	**Countdown Type Status** — RO. This bit reflects the current countdown type. 0 = Binary countdown 1 = Binary Coded Decimal (BCD) countdown.

7.3.3 Counter Access Ports Register

I/O Address: Counter 0 – 40h, Counter 1 – 41h, Counter 2 – 42h
Attribute: R/W
Default Value: All bits undefined
Size: 8 bits

Bit	Description
7:0	**Counter Port** — R/W. Each counter port address is used to program the 16-bit Count Register. The order of programming, either LSB only, MSB only, or LSB then MSB, is defined with the Interval Counter Control Register at port 43h. The counter port is also used to read the current count from the Count Register, and return the status of the counter programming following a Read Back Command.

7.4 8259 Interrupt Controller (PIC) Registers

7.4.1 Interrupt Controller I/O MAP

The interrupt controller registers are located at 20h and 21h for the master controller (IRQ 0–7), and at A0h and A1h for the slave controller (IRQ 8–13). These registers have multiple functions, depending upon the data written to them. Table 7-3 shows the different register possibilities for each address.

Table 7-3. PIC Registers

Port	Aliases	Register Name	Default Value	Type
20h	24h, 28h, 2Ch, 30h, 34h, 38h, 3Ch	Master PIC ICW1 Init. Cmd Word 1	Undefined	WO
		Master PIC OCW2 Op Ctrl Word 2	001XXXXXb	WO
		Master PIC OCW3 Op Ctrl Word 3	X01XXX10b	WO
21h	25h, 29h, 2Dh, 31h, 35h, 39h, 3Dh	Master PIC ICW2 Init. Cmd Word 2	Undefined	WO
		Master PIC ICW3 Init. Cmd Word 3	Undefined	WO
		Master PIC ICW4 Init. Cmd Word 4	01h	WO
		Master PIC OCW1 Op Ctrl Word 1	00h	R/W
A0h	A4h, A8h, ACh, B0h, B4h, B8h, BCh	Slave PIC ICW1 Init. Cmd Word 1	Undefined	WO
		Slave PIC OCW2 Op Ctrl Word 2	001XXXXXb	WO
		Slave PIC OCW3 Op Ctrl Word 3	X01XXX10b	WO

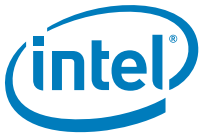


Table 7-3. PIC Registers

Port	Aliases	Register Name	Default Value	Type
A1h	A5h, A9h, ADh, B1h, B5h, B9h, BDh	Slave PIC ICW2 Init. Cmd Word 2	Undefined	WO
		Slave PIC ICW3 Init. Cmd Word 3	Undefined	WO
		Slave PIC ICW4 Init. Cmd Word 4	01h	WO
		Slave PIC OCW1 Op Ctrl Word 1	00h	R/W
4D0h	–	Master PIC Edge/Level Triggered	00h	R/W
4D1h	–	Slave PIC Edge/Level Triggered	00h	R/W

Note: Refer to note addressing active-low interrupt sources in 8259 Interrupt Controllers section (Section 3.8).

7.4.2 ICW1—Initialization Command Word 1 Register

Offset Address: Master Controller – 20h / Slave Controller – A0h
Attribute: WO
Size: 8 bits /controller
Default Value: All bits undefined

A write to Initialization Command Word 1 starts the interrupt controller initialization sequence, during which the following occurs:

1. The Interrupt Mask register is cleared.
2. IRQ7 input is assigned priority 7.
3. The slave mode address is set to 7.
4. Special mask mode is cleared and Status Read is set to IRR.

Once this write occurs, the controller expects writes to ICW2, ICW3, and ICW4 to complete the initialization sequence.

Bit	Description
7:5	**ICW/OCW Select** — WO. These bits are MCS-85 specific, and not needed. 000 = Should be programmed to "000"
4	**ICW/OCW Select** — WO. 1 = This bit must be a 1 to select ICW1 and enable the ICW2, ICW3, and ICW4 sequence.
3	**Edge/Level Bank Select (LTIM)** — WO. Disabled. Replaced by the edge/level triggered control registers (ELCR, D31:F0:4D0h, D31:F0:4D1h).
2	ADI — WO. 0 = Ignored for Intel® Xeon® Processor D-1500 Product Family. Should be programmed to 0.
1	**Single or Cascade (SNGL)** — WO. 0 = Must be programmed to a 0 to indicate two controllers operating in cascade mode.
0	**ICW4 Write Required (IC4)** — WO. 1 = This bit must be programmed to a 1 to indicate that ICW4 needs to be programmed.

7.4.3 ICW2—Initialization Command Word 2 Register

Offset Address:	Master Controller – 21h Slave Controller – A1h	Attribute:	WO
		Size:	8 bits /controller
Default Value:	All bits undefined		

ICW2 is used to initialize the interrupt controller with the five most significant bits of the interrupt vector address. The value programmed for bits[7:3] is used by the processor to define the base address in the interrupt vector table for the interrupt routines associated with each IRQ on the controller. Typical ISA ICW2 values are 08h for the master controller and 70h for the slave controller.

Bit	Description
7:3	**Interrupt Vector Base Address** — WO. Bits [7:3] define the base address in the interrupt vector table for the interrupt routines associated with each interrupt request level input.
2:0	**Interrupt Request Level** — WO. When writing ICW2, these bits should all be 0. During an interrupt acknowledge cycle, these bits are programmed by the interrupt controller with the interrupt to be serviced. This is combined with bits [7:3] to form the interrupt vector driven onto the data bus during the second INTA# cycle. The code is a three bit binary code: **Code** — **Master Interrupt** — **Slave Interrupt** 000b — IRQ0 — IRQ8 001b — IRQ1 — IRQ9 010b — IRQ2 — IRQ10 011b — IRQ3 — IRQ11 100b — IRQ4 — IRQ12 101b — IRQ5 — IRQ13 110b — IRQ6 — IRQ14 111b — IRQ7 — IRQ15

7.4.4 ICW3—Master Controller Initialization Command Word 3 Register

Offset Address:	21h	Attribute:	WO
Default Value:	All bits undefined	Size:	8 bits

Bit	Description
7:3	0 = These bits must be programmed to 0.
2	**Cascaded Interrupt Controller IRQ Connection** — WO. This bit indicates that the slave controller is cascaded on IRQ2. When IRQ8#–IRQ15 is asserted, it goes through the slave controller's priority resolver. The slave controller's INTR output onto IRQ2. IRQ2 then goes through the master controller's priority solver. If it wins, the INTR signal is asserted to the processor, and the returning interrupt acknowledge returns the interrupt vector for the slave controller. 1 = This bit must always be programmed to a 1.
1:0	0 = These bits must be programmed to 0.

7.4.5 ICW3—Slave Controller Initialization Command Word 3 Register

Offset Address: A1h
Attribute: WO
Default Value: All bits undefined
Size: 8 bits

Bit	Description
7:3	0 = These bits must be programmed to 0.
2:0	**Slave Identification Code** — WO. These bits are compared against the slave identification code broadcast by the master controller from the trailing edge of the first internal INTA# pulse to the trailing edge of the second internal INTA# pulse. These bits must be programmed to 02h to match the code broadcast by the master controller. When 02h is broadcast by the master controller during the INTA# sequence, the slave controller assumes responsibility for broadcasting the interrupt vector.

7.4.6 ICW4—Initialization Command Word 4 Register

Offset Address: Master Controller – 021h
Slave Controller – 0A1h
Attribute: WO
Size: 8 bits
Default Value: 01h

Bit	Description
7:5	0 = These bits must be programmed to 0.
4	**Special Fully Nested Mode (SFNM)** — WO. 0 = Should normally be disabled by writing a 0 to this bit. 1 = Special fully nested mode is programmed.
3	**Buffered Mode (BUF)** — WO. 0 = Must be programmed to 0 for Intel® Xeon® Processor D-1500 Product Family. This is non-buffered mode.
2	**Master/Slave in Buffered Mode** — WO. Not used. 0 = Should always be programmed to 0.
1	**Automatic End of Interrupt (AEOI)** — WO. 0 = This bit should normally be programmed to 0. This is the normal end of interrupt. 1 = Automatic End of Interrupt (AEOI) mode is programmed.
0	**Microprocessor Mode** — WO. 1 = Must be programmed to 1 to indicate that the controller is operating in an Intel Architecture-based system.

7.4.7 OCW1—Operational Control Word 1 (Interrupt Mask) Register

Offset Address: Master Controller – 021h
Slave Controller – 0A1h
Attribute: R/W
Size: 8 bits
Default Value: 00h

Bit	Description
7:0	**Interrupt Request Mask** — R/W. When a 1 is written to any bit in this register, the corresponding IRQ line is masked. When a 0 is written to any bit in this register, the corresponding IRQ mask bit is cleared, and interrupt requests will again be accepted by the controller. Masking IRQ2 on the master controller will also mask the interrupt requests from the slave controller.

7.4.8 OCW2—Operational Control Word 2 Register

Offset Address: Master Controller – 020h; Slave Controller – 0A0h
Attribute: WO
Size: 8 bits
Default Value: Bit[4:0]=undefined, Bit[7:5]=001

Following a part reset or ICW initialization, the controller enters the fully nested mode of operation. Non-specific EOI without rotation is the default. Both rotation mode and specific EOI mode are disabled following initialization.

Bit	Description
7:5	**Rotate and EOI Codes** (R, SL, EOI) — WO. These three bits control the Rotate and End of Interrupt modes and combinations of the two. 000 = Rotate in Auto EOI Mode (Clear) 001 = Non-specific EOI command 010 = No Operation 011 = *Specific EOI Command 100 = Rotate in Auto EOI Mode (Set) 101 = Rotate on Non-Specific EOI Command 110 = *Set Priority Command 111 = *Rotate on Specific EOI Command *L0 – L2 Are Used
4:3	**OCW2 Select** — WO. When selecting OCW2, bits 4:3 = 00
2:0	**Interrupt Level Select** (L2, L1, L0) — WO. L2, L1, and L0 determine the interrupt level acted upon when the SL bit is active. A simple binary code, outlined below, selects the channel for the command to act upon. When the SL bit is inactive, these bits do not have a defined function; programming L2, L1 and L0 to 0 is sufficient in this case. **Code / Interrupt Level / Code / Interrupt Level** 000b IRQ0/8 000b IRQ4/12 001b IRQ1/9 001b IRQ5/13 010b IRQ2/10 010b IRQ6/14 011b IRQ3/11 011b IRQ7/15

7.4.9 OCW3—Operational Control Word 3 Register

Offset Address: Master Controller – 020h; Slave Controller – 0A0h
Attribute: WO
Size: 8 bits
Default Value: Bit[6,0]=0, Bit[7,4:2]=undefined, Bit[5,1]=1

Bit	Description
7	Reserved. Must be 0.
6	**Special Mask Mode (SMM)** — WO. 1 = The Special Mask Mode can be used by an interrupt service routine to dynamically alter the system priority structure while the routine is executing, through selective enabling/disabling of the other channel's mask bits. Bit 5, the ESMM bit, must be set for this bit to have any meaning.
5	**Enable Special Mask Mode (ESMM)** — WO. 0 = Disable. The SMM bit becomes a "don't care". 1 = Enable the SMM bit to set or reset the Special Mask Mode.
4:3	**OCW3 Select** — WO. When selecting OCW3, bits 4:3 = 01
2	**Poll Mode Command** — WO. 0 = Disable. Poll Command is not issued. 1 = Enable. The next I/O read to the interrupt controller is treated as an interrupt acknowledge cycle. An encoded byte is driven onto the data bus, representing the highest priority level requesting service.

Bit	Description
1:0	**Register Read Command** — WO. These bits provide control for reading the In-Service Register (ISR) and the Interrupt Request Register (IRR). When bit 1=0, bit 0 will not affect the register read selection. When bit 1=1, bit 0 selects the register status returned following an OCW3 read. If bit 0=0, the IRR will be read. If bit 0=1, the ISR will be read. Following ICW initialization, the default OCW3 port address read will be "read IRR". To retain the current selection (read ISR or read IRR), always write a 0 to bit 1 when programming this register. The selected register can be read repeatedly without reprogramming OCW3. To select a new status register, OCW3 must be reprogrammed prior to attempting the read. 00 = No Action 01 = No Action 10 = Read IRQ Register 11 = Read IS Register

7.4.10 ELCR1—Master Controller Edge/Level Triggered Register

Offset Address: 4D0h Attribute: R/W
Default Value: 00h Size: 8 bits

In edge mode, (bit[x] = 0), the interrupt is recognized by a low to high transition. In level mode (bit[x] = 1), the interrupt is recognized by a high level. The cascade channel, IRQ2, the heart beat timer (IRQ0), and the keyboard controller (IRQ1), cannot be put into level mode.

Bit	Description
7	**IRQ7 ECL** — R/W. 0 = Edge 1 = Level
6	**IRQ6 ECL** — R/W. 0 = Edge 1 = Level
5	**IRQ5 ECL** — R/W. 0 = Edge 1 = Level
4	**IRQ4 ECL** — R/W. 0 = Edge 1 = Level
3	**IRQ3 ECL** — R/W. 0 = Edge 1 = Level
2:0	Reserved. Must be 0.

7.4.11 ELCR2—Slave Controller Edge/Level Triggered Register

Offset Address: 4D1h
Attribute: R/W
Default Value: 00h
Size: 8 bits

In edge mode, (bit[x] = 0), the interrupt is recognized by a low to high transition. In level mode (bit[x] = 1), the interrupt is recognized by a high level. The real time clock, IRQ8#, and the floating point error interrupt, IRQ13, cannot be programmed for level mode.

Bit	Description
7	**IRQ15 ECL** — R/W. 0 = Edge 1 = Level
6	**IRQ14 ECL** — R/W. 0 = Edge 1 = Level
5	Reserved. Must be 0.
4	**IRQ12 ECL** — R/W. 0 = Edge 1 = Level
3	**IRQ11 ECL** — R/W. 0 = Edge 1 = Level
2	**IRQ10 ECL** — R/W. 0 = Edge 1 = Level
1	**IRQ9 ECL** — R/W. 0 = Edge 1 = Level
0	Reserved. Must be 0.

7.5 Advanced Programmable Interrupt Controller (APIC)

7.5.1 APIC Register Map

The APIC is accessed using an indirect addressing scheme. Two registers are visible by software for manipulation of most of the APIC registers. These registers are mapped into memory space. The address bits 19:12 of the address range are programmable through bits 7:0 of OIC register (Chipset Config Registers:Offset 31FEh) The registers are shown in Table 7-4.

Table 7-4. APIC Direct Registers

Address	Mnemonic	Register Name	Size	Type
FEC_ _0000h	IND	Index	8 bits	R/W
FEC_ _0010h	DAT	Data	32 bits	R/W
FEC_ _0040h	EOIR	EOI	32 bits	WO

Table 7-5 lists the registers that can be accessed within the APIC using the Index Register. When accessing these registers, accesses must be done one DWord at a time. For example, software should never access byte 2 from the Data register before accessing bytes 0 and 1. The hardware will not attempt to recover from a bad programming model in this case.

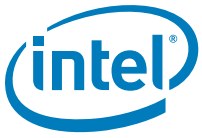


Table 7-5. APIC Indirect Registers

Index	Mnemonic	Register Name	Size	Type
00	ID	Identification	32 bits	R/W
01	VER	Version	32 bits	RO
02–0F	—	Reserved	—	RO
10–11	REDIR_TBL0	Redirection Table 0	64 bits	R/W, RO
12–13	REDIR_TBL1	Redirection Table 1	64 bits	R/W, RO
...	...	...	...	...
3E–3F	REDIR_TBL23	Redirection Table 23	64 bits	R/W, RO
40–FF	—	Reserved	—	RO

7.5.2 IND—Index Register

Memory Address FEC_ _0000h Attribute: R/W
Default Value: 00h Size: 8 bits

The Index Register will select which APIC indirect register to be manipulated by software. The selector values for the indirect registers are listed in Table 7-5. Software will program this register to select the desired APIC internal register.

Bit	Description
7:0	**APIC Index** — R/W. This is an 8-bit pointer into the I/O APIC register table.

7.5.3 DAT—Data Register

Memory Address FEC_ _0000h Attribute: R/W
Default Value: 00000000h Size: 32 bits

This is a 32-bit register specifying the data to be read or written to the register pointed to by the Index register. This register can only be accessed in DWord quantities.

Bit	Description
7:0	**APIC Data** — R/W. This is a 32-bit register for the data to be read or written to the APIC indirect register (Figure 7-5) pointed to by the Index register (Memory Address FEC0_0000h).

7.5.4 EOIR—EOI Register

Memory Address FEC_ _0000h Attribute: R/W
Default Value: N/A Size: 32 bits

The EOI register is present to provide a mechanism to maintain the level triggered semantics for level-triggered interrupts issued on the parallel bus.

When a write is issued to this register, the I/O APIC will check the lower 8 bits written to this register, and compare it with the vector field for each entry in the I/O Redirection Table. When a match is found, the Remote_IRR bit (Index Offset 10h, bit 14) for that I/O Redirection Entry will be cleared.

Note: If multiple I/O Redirection entries, for any reason, assign the same vector for more than one interrupt input, each of those entries will have the Remote_IRR bit reset to 0. The interrupt, which was prematurely reset, will not be lost because if its input remained active when the Remote_IRR bit was cleared, the interrupt will be reissued

and serviced at a later time. Only bits 7:0 are actually used. Bits 31:8 are ignored by Intel® Xeon® Processor D-1500 Product Family.

Note: To provide for future expansion, the processor should always write a value of 0 to Bits 31:8.

Bit	Description
31:8	Reserved. To provide for future expansion, the processor should always write a value of 0 to Bits 31:8.
7:0	**Redirection Entry Clear** — WO. When a write is issued to this register, the I/O APIC will check this field, and compare it with the vector field for each entry in the I/O Redirection Table. When a match is found, the Remote_IRR bit for that I/O Redirection Entry will be cleared.

7.5.5 ID—Identification Register

Index Offset: 00h Attribute: R/W
Default Value: 00000000h Size: 32 bits

The APIC ID serves as a physical name of the APIC. The APIC bus arbitration ID for the APIC is derived from its I/O APIC ID. This register is reset to 0 on power-up reset.

Bit	Description
31:28	Reserved
27:24	**APIC ID** — R/W. Software must program this value before using the APIC.
23:16	Reserved
15	Scratchpad Bit
14:0	Reserved

7.5.6 VER—Version Register

Index Offset: 01h Attribute: RO, R/WO
Default Value: 00170020h Size: 32 bits

Each I/O APIC contains a hardwired Version Register that identifies different implementation of APIC and their versions. The maximum redirection entry information also is in this register, to let software know how many interrupt are supported by this APIC.

Bit	Description
31:24	Reserved
23:16	**Maximum Redirection Entries (MRE)** — R/WO. This is the entry number (0 being the lowest entry) of the highest entry in the redirection table. It is equal to the number of interrupt input pins minus one and is in the range 0 through 239. In Intel® Xeon® Processor D-1500 Product Family this field is hardwired to 17h to indicate 24 interrupts. BIOS must write to this field after PLTRST# to lockdown the value. this allows BIOS to utilize some of the entries for its own purpose and thus advertising fewer IOxAPIC Redirection Entries to the OS.
15	**Pin Assertion Register Supported (PRQ)** — RO. Indicate that the IOxAPIC does not implement the Pin Assertion Register.
14:8	Reserved
7:0	**Version (VS)** — RO. This is a version number that identifies the implementation version.

7.5.7 REDIR_TBL—Redirection Table Register

Index Offset:	10h–11h (vector 0) through 3E–3Fh (vector 23)	Attribute:	R/W, RO
Default Value:	Bit 16 = 1. All other bits undefined	Size:	64 bits each, (accessed as two 32 bit quantities)

The Redirection Table has a dedicated entry for each interrupt input pin. The information in the Redirection Table is used to translate the interrupt manifestation on the corresponding interrupt pin into an APIC message.

The APIC will respond to an edge triggered interrupt as long as the interrupt is held until after the acknowledge cycle has begun. Once the interrupt is detected, a delivery status bit internally to the I/O APIC is set. The state machine will step ahead and wait for an acknowledgment from the APIC unit that the interrupt message was sent. Only then will the I/O APIC be able to recognize a new edge on that interrupt pin. That new edge will only result in a new invocation of the handler if its acceptance by the destination APIC causes the Interrupt Request Register bit to go from 0 to 1. (In other words, if the interrupt was not already pending at the destination.)

Bit	Description
63:56	**Destination** — R/W. If bit 11 of this entry is 0 (Physical), then bits 59:56 specifies an APIC ID. In this case, bits 63:59 should be programmed by software to 0. If bit 11 of this entry is 1 (Logical), then bits 63:56 specify the logical destination address of a set of processors.
55:48	**Extended Destination ID (EDID)** — RO. These bits are sent to a local APIC only when in Processor System Bus mode. They become bits 11:4 of the address.
47:17	Reserved
16	**Mask** — R/W. 0 = Not masked: An edge or level on this interrupt pin results in the delivery of the interrupt to the destination. 1 = Masked: Interrupts are not delivered nor held pending. Setting this bit after the interrupt is accepted by a local APIC has no effect on that interrupt. This behavior is identical to the device withdrawing the interrupt before it is posted to the processor. It is software's responsibility to deal with the case where the mask bit is set after the interrupt message has been accepted by a local APIC unit but before the interrupt is dispensed to the processor.
15	**Trigger Mode** — R/W. This field indicates the type of signal on the interrupt pin that triggers an interrupt. 0 = Edge triggered. 1 = Level triggered.
14	**Remote IRR** — R/W. This bit is used for level triggered interrupts; its meaning is undefined for edge triggered interrupts. 0 = Reset when an EOI message is received from a local APIC. 1 = Set when Local APIC/s accept the level interrupt sent by the I/O APIC.
13	**Interrupt Input Pin Polarity** — R/W. This bit specifies the polarity of each interrupt signal connected to the interrupt pins. 0 = Active high. 1 = Active low.
12	**Delivery Status** — RO. This field contains the current status of the delivery of this interrupt. Writes to this bit have no effect. 0 = Idle. No activity for this interrupt. 1 = Pending. Interrupt has been injected, but delivery is not complete.
11	**Destination Mode** — R/W. This field determines the interpretation of the Destination field. 0 = Physical. Destination APIC ID is identified by bits 59:56. 1 = Logical. Destinations are identified by matching bit 63:56 with the Logical Destination in the Destination Format Register and Logical Destination Register in each Local APIC.
10:8	**Delivery Mode** — R/W. This field specifies how the APICs listed in the destination field should act upon reception of this signal. Certain Delivery Modes will only operate as intended when used in conjunction with a specific trigger mode. These encodings are listed in the note below:

Bit	Description
7:0	**Vector** — R/W. This field contains the interrupt vector for this interrupt. Values range between 10h and FEh.

Note: Delivery Mode encoding:

000 = Fixed. Deliver the signal on the INTR signal of all processor cores listed in the destination. Trigger Mode can be edge or level.

001 = Lowest Priority. Deliver the signal on the INTR signal of the processor core that is executing at the lowest priority among all the processors listed in the specified destination. Trigger Mode can be edge or level.

010 = SMI (System Management Interrupt). Requires the interrupt to be programmed as edge triggered. The vector information is ignored but must be programmed to all 0s for future compatibility: **not supported**

011 = Reserved

100 = NMI. Deliver the signal on the NMI signal of all processor cores listed in the destination. Vector information is ignored. NMI is treated as an edge triggered interrupt even if it is programmed as level triggered. For proper operation this redirection table entry must be programmed to edge triggered. The NMI delivery mode does not set the RIRR bit. If the redirection table is incorrectly set to level, the loop count will continue counting through the redirection table addresses. Once the count for the NMI pin is reached again, the interrupt will be sent again: **not supported**

101 = INIT. Deliver the signal to all processor cores listed in the destination by asserting the INIT signal. All addressed local APICs will assume their INIT state. INIT is always treated as an edge triggered interrupt even if programmed as level triggered. For proper operation this redirection table entry must be programmed to edge triggered. The INIT delivery mode does not set the RIRR bit. If the redirection table is incorrectly set to level, the loop count will continue counting through the redirection table addresses. Once the count for the INIT pin is reached again, the interrupt will be sent again: **not supported**

110 = Reserved

111 = ExtINT. Deliver the signal to the INTR signal of all processor cores listed in the destination as an interrupt that originated in an externally connected 8259A compatible interrupt controller. The INTA cycle that corresponds to this ExtINT delivery will be routed to the external controller that is expected to supply the vector. Requires the interrupt to be programmed as edge triggered.

7.6 Real Time Clock Registers

7.6.1 I/O Register Address Map

The RTC internal registers and RAM are organized as two banks of 128 bytes each, called the standard and extended banks. The first 14 bytes of the standard bank contain the RTC time and date information along with four registers, A–D, that are used for configuration of the RTC. The extended bank contains a full 128 bytes of battery backed SRAM, and will be accessible even when the RTC module is disabled (using the RTC configuration register). Registers A–D do not physically exist in the RAM.

All data movement between the host processor and the real-time clock is done through registers mapped to the standard I/O space. The register map is shown in Table 7-6.

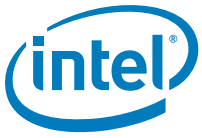


Table 7-6. RTC I/O Registers

I/O Locations	If U128E bit = 0	Function
70h and 74h	Also alias to 72h and 76h	Real-Time Clock (Standard RAM) Index Register
71h and 75h	Also alias to 73h and 77h	Real-Time Clock (Standard RAM) Target Register
72h and 76h		Extended RAM Index Register (if enabled)
73h and 77h		Extended RAM Target Register (if enabled)

Notes:

1. I/O locations 70h and 71h are the standard legacy location for the real-time clock. The map for this bank is shown in Table 7-7. Locations 72h and 73h are for accessing the extended RAM. The extended RAM bank is also accessed using an indexed scheme. I/O address 72h is used as the address pointer and I/O address 73h is used as the data register. Index addresses above 127h are not valid. If the extended RAM is not needed, it may be disabled.
2. Software must preserve the value of bit 7 at I/O addresses 70h and 74h. When writing to this address, software must first read the value, and then write the same value for bit 7 during the sequential address write. Port 70h is not directly readable. The only way to read this register is through Alt Access mode. Although RTC Index bits 6:0 are readable from port 74h, bit 7 will always return 0. If the NMI# enable is not changed during normal operation, software can alternatively read this bit once and then retain the value for all subsequent writes to port 70h.

7.6.2 Indexed Registers

The RTC contains two sets of indexed registers that are accessed using the two separate Index and Target registers (70/71h or 72/73h), as shown in Table 7-7.

Table 7-7. RTC (Standard) RAM Bank

Index	Name
00h	Seconds
01h	Seconds Alarm
02h	Minutes
03h	Minutes Alarm
04h	Hours
05h	Hours Alarm
06h	Day of Week
07h	Day of Month
08h	Month
09h	Year
0Ah	Register A
0Bh	Register B
0Ch	Register C
0Dh	Register D
0Eh–7Fh	114 Bytes of User RAM

7.6.2.1 RTC_REGA—Register A

RTC Index:	0A	Attribute:	R/W
Default Value:	Undefined	Size:	8 bits
Lockable:	No	Power Well:	RTC

This register is used for general configuration of the RTC functions. None of the bits are affected by RSMRST# or any other Intel® Xeon® Processor D-1500 Product Family reset signal.

Bit	Description
7	**Update In Progress (UIP)** — R/W. This bit may be monitored as a status flag. 0 = The update cycle will not start for at least 488 µs. The time, calendar, and alarm information in RAM is always available when the UIP bit is 0. 1 = The update is soon to occur or is in progress.
6:4	**Division Chain Select (DV[2:0])** — R/W. These three bits control the divider chain for the oscillator, and are not affected by RSMRST# or any other reset signal. 010 = Normal Operation 11X = Divider Reset 101 = Bypass 15 stages (test mode only) 100 = Bypass 10 stages (test mode only) 011 = Bypass 5 stages (test mode only) 001 = Invalid 000 = Invalid
3:0	**Rate Select (RS[3:0])** — R/W. Selects one of 13 taps of the 15 stage divider chain. The selected tap can generate a periodic interrupt if the PIE bit is set in Register B. Otherwise this tap will set the PF flag of Register C. If the periodic interrupt is not to be used, these bits should all be cleared to 0. RS3 corresponds to bit 3. 0000 = Interrupt never toggles 0001 = 3.90625 ms 0010 = 7.8125 ms 0011 = 122.070 µs 0100 = 244.141 µs 0101 = 488.281 µs 0110 = 976.5625 µs 0111 = 1.953125 ms 1000 = 3.90625 ms 1001 = 7.8125 ms 1010 = 15.625 ms 1011 = 31.25 ms 1100 = 62.5 ms 1101 = 125 ms 1110 = 250 ms 1111= 500 ms

7.6.2.2 RTC_REGB—Register B (General Configuration)

RTC Index:	0Bh	Attribute:	R/W
Default Value:	U0U00UUU (U: Undefined)	Size:	8 bits
Lockable:	No	Power Well:	RTC

Bit	Description
7	**Update Cycle Inhibit (SET)** — R/W. Enables/Inhibits the update cycles. This bit is not affected by RSMRST# nor any other reset signal. 0 = Update cycle occurs normally once each second. 1 = A current update cycle will abort and subsequent update cycles will not occur until SET is returned to 0. When set is one, the BIOS may initialize time and calendar bytes safely. ***Note:*** This bit should be set then cleared early in BIOS POST after each powerup directly after coin-cell battery insertion.

Bit	Description
6	**Periodic Interrupt Enable (PIE)** — R/W. This bit is cleared by RSMRST#, but not on any other reset. 0 = Disable. 1 = Enable. Allows an interrupt to occur with a time base set with the RS bits of register A.
5	**Alarm Interrupt Enable (AIE)** — R/W. This bit is cleared by RTCRST#, but not on any other reset. 0 = Disable. 1 = Enable. Allows an interrupt to occur when the AF is set by an alarm match from the update cycle. An alarm can occur once a second, one an hour, once a day, or one a month.
4	**Update-Ended Interrupt Enable (UIE)** — R/W. This bit is cleared by RSMRST#, but not on any other reset. 0 = Disable. 1 = Enable. Allows an interrupt to occur when the update cycle ends.
3	**Square Wave Enable (SQWE)** — R/W. This bit serves no function in Intel® Xeon® Processor D-1500 Product Family. It is left in this register bank to provide compatibility with the Motorola 146818B*. Intel® Xeon® Processor D-1500 Product Family has no SQW pin. This bit is cleared by RSMRST#, but not on any other reset.
2	**Data Mode (DM)** — R/W. This bit specifies either binary or BCD data representation. This bit is not affected by RSMRST# nor any other reset signal. 0 = BCD 1 = Binary
1	**Hour Format (HOURFORM)** — R/W. This bit indicates the hour byte format. This bit is not affected by RSMRST# nor any other reset signal. 0 = Twelve-hour mode. In twelve-hour mode, the seventh bit represents AM as 0 and PM as one. 1 = Twenty-four hour mode.
0	**Daylight Savings Legacy Software Support (DSLSWS)** — R/W. Daylight savings functionality is no longer supported. This bit is used to maintain legacy software support and has no associated functionality. If BUC.DSO bit is set, the DSLSWS bit continues to be R/W.

7.6.2.3 RTC_REGC—Register C (Flag Register)

RTC Index:	0Ch	Attribute:	RO
Default Value:	00U00000 (U: Undefined)	Size:	8 bits
Lockable:	No	Power Well:	RTC

Writes to Register C have no effect.

Bit	Description
7	**Interrupt Request Flag (IRQF)** — RO. IRQF = (PF * PIE) + (AF * AIE) + (UF *UFE). This bit also causes the RTC Interrupt to be asserted. This bit is cleared upon RSMRST# or a read of Register C.
6	**Periodic Interrupt Flag (PF)** — RO. This bit is cleared upon RSMRST# or a read of Register C. 0 = If no taps are specified using the RS bits in Register A, this flag will not be set. 1 = Periodic interrupt Flag will be 1 when the tap specified by the RS bits of register A is 1.
5	**Alarm Flag (AF)** — RO. 0 = This bit is cleared upon RTCRST# or a read of Register C. 1 = Alarm Flag will be set after all Alarm values match the current time.
4	**Update-Ended Flag (UF)** — RO. 0 = The bit is cleared upon RSMRST# or a read of Register C. 1 = Set immediately following an update cycle for each second.
3:0	Reserved. Will always report 0.

7.6.2.4 RTC_REGD—Register D (Flag Register)

RTC Index:	0Dh	Attribute:	R/W
Default Value:	10UUUUUU (U: Undefined)	Size:	8 bits
Lockable:	No	Power Well:	RTC

Bit	Description
7	**Valid RAM and Time Bit (VRT)** — R/W. 0 = This bit should always be written as a 0 for write cycle, however it will return a 1 for read cycles. 1 = This bit is hardwired to 1 in the RTC power well.
6	Reserved. This bit always returns a 0 and should be cleared to 0 for write cycles.
5:0	**Date Alarm** — R/W. These bits store the date of month alarm value. If set to 000000b, then a don't care state is assumed. The host must configure the date alarm for these bits to do anything, yet they can be written at any time. If the date alarm is not enabled, these bits will return 0s to mimic the functionality of the Motorola 146818B*. These bits are not affected by any reset assertion.

7.7 Processor Interface Registers

Table 7-8 is the register address map for the processor interface registers.

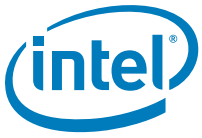
Table 7-8. Processor Interface PCI Register Address Map

Offset	Mnemonic	Register Name	Default	Attribute
61h	NMI_SC	NMI Status and Control	00h	R/W, RO
70h	NMI_EN	NMI Enable	80h	R/W (special)
92h	PORT92	Init	00h	R/W
F0h	COPROC_ERR	Coprocessor Error	00h	WO
CF9h	RST_CNT	Reset Control	00h	R/W

7.7.1 NMI_SC—NMI Status and Control Register

I/O Address:	61h	Attribute:	R/W, RO
Default Value:	00h	Size:	8 bits
Lockable:	No	Power Well:	Core

Bit	Description
7	**SERR# NMI Source Status (SERR#_NMI_STS)** — RO. 1 = Bit is set if a PCI agent detected a system error and pulses the PCI SERR# line and if bit 2 (PCI_SERR_EN) is cleared. This interrupt source is enabled by setting bit 2 to 0. To reset the interrupt, set bit 2 to 1 and then set it to 0. When writing to port 61h, this bit must be 0. ***Note:*** This bit is set by any of Intel® Xeon® Processor D-1500 Product Family internal sources of SERR; this includes SERR assertions forwarded from the secondary PCI bus, errors on a PCI Express* port, or other internal functions that generate SERR#.
6	**IOCHK# NMI Source Status (IOCHK_NMI_STS)** — RO. 1 = Bit is set if an LPC agent (using SERIRQ) asserted IOCHK# and if bit 3 (IOCHK_NMI_EN) is cleared. This interrupt source is enabled by setting bit 3 to 0. To reset the interrupt, set bit 3 to 1 and then set it to 0. When writing to port 61h, this bit must be a 0.
5	**Timer Counter 2 OUT Status (TMR2_OUT_STS)** — RO. This bit reflects the current state of the 8254 counter 2 output. Counter 2 must be programmed following any PCI reset for this bit to have a determinate value. When writing to port 61h, this bit must be a 0.
4	**Refresh Cycle Toggle (REF_TOGGLE)** — RO. This signal toggles from either 0 to 1 or 1 to 0 at a rate that is equivalent to when refresh cycles would occur. When writing to port 61h, this bit must be a 0.
3	**IOCHK# NMI Enable (IOCHK_NMI_EN)** — R/W. 0 = Enabled. 1 = Disabled and cleared.
2	**PCI SERR# Enable (PCI_SERR_EN)** — R/W. 0 = SERR# NMIs are enabled. 1 = SERR# NMIs are disabled and cleared.



Bit	Description
1	**Speaker Data Enable (SPKR_DAT_EN)** — R/W. 0 = SPKR output is a 0. 1 = SPKR output is equivalent to the Counter 2 OUT signal value.
0	**Timer Counter 2 Enable (TIM_CNT2_EN)** — R/W. 0 = Disable 1 = Enable

7.7.2 NMI_EN—NMI Enable (and Real Time Clock Index) Register

I/O Address:	70h	Attribute:	R/W (special)
Default Value:	80h	Size:	8 bits
Lockable:	No	Power Well:	Core

Note: The RTC Index field is write-only for normal operation. This field can only be read in Alt-Access Mode. Note, however, that this register is aliased to Port 74h (documented in Table 7-6), and all bits are readable at that address.

Bits	Description
7	**NMI Enable (NMI_EN)** — R/W (special). 0 = Enable NMI sources. 1 = Disable All NMI sources.
6:0	**Real Time Clock Index Address (RTC_INDX)** — R/W (special). This data goes to the RTC to select which register or CMOS RAM address is being accessed.

7.7.3 PORT92—Init Register

I/O Address:	92h	Attribute:	R/W
Default Value:	00h	Size:	8 bits
Lockable:	No	Power Well:	Core

Bit	Description
7:2	Reserved
1	**Alternate A20 Gate (ALT_A20_GATE)** — R/W. Functionality reserved. A20M# functionality is not supported.
0	**INIT_NOW** — R/W. When this bit transitions from a 0 to a 1, Intel® Xeon® Processor D-1500 Product Family will force INIT# active for 16 PCI clocks.

7.7.4 COPROC_ERR—Coprocessor Error Register

I/O Address:	F0h	Attribute:	WO
Default Value:	00h	Size:	8 bits
Lockable:	No	Power Well:	Core

Bits	Description
7:0	**Coprocessor Error (COPROC_ERR)** — WO. Any value written to this register will cause IGNNE# to go active, if FERR# had generated an internal IRQ13. For FERR# to generate an internal IRQ13, the COPROC_ERR_EN bit must be 1.

7.7.5 RST_CNT—Reset Control Register

I/O Address:	CF9h	Attribute:	R/W
Default Value:	00h	Size:	8 bits
Lockable:	No	Power Well:	Core

Bit	Description
7:4	Reserved
3	**Full Reset (FULL_RST)** — R/W. This bit is used to determine the states of SLP_S3#, SLP_S4#, and SLP_S5# after a CF9 hard reset (SYS_RST =1 and RST_CPU is set to 1), after PCH_PWROK going low (with RSMRST# high), or after two TCO timeouts. 0 = Intel® Xeon® Processor D-1500 Product Family will keep SLP_S3#, SLP_S4# and SLP_S5# high. 1 = Intel® Xeon® Processor D-1500 Product Family will drive SLP_S3#, SLP_S4# and SLP_S5# low for 3–5 seconds. ***Note:*** When this bit is set, it also causes the full power cycle (SLP_S3/4/5# assertion) in response to SYS_RESET#, PWROK#, and Watchdog timer reset sources.
2	**Reset Processor (RST_CPU)** — R/W. When this bit transitions from a 0 to a 1, it initiates a hard or soft reset, as determined by the SYS_RST bit (bit 1 of this register).
1	**System Reset (SYS_RST)** — R/W. This bit is used to determine a hard or soft reset to the processor. 0 = When RST_CPU bit goes from 0 to 1, Intel® Xeon® Processor D-1500 Product Family performs a soft reset by activating INIT# for 16 PCI clocks. 1 = When RST_CPU bit goes from 0 to 1, Intel® Xeon® Processor D-1500 Product Family performs a hard reset by activating PLTRST# and SUS_STAT# active for a minimum of about 1 milliseconds. In this case, SLP_S3#, SLP_S4# and SLP_S5# state (assertion or de-assertion) depends on FULL_RST bit setting. Intel® Xeon® Processor D-1500 Product Family main power well is reset when this bit is 1. It also resets the resume well bits (except for those noted throughout this document).
0	Reserved

7.8 Power Management Registers

The power management registers are distributed within the PCI Device 31: Function 0 space, as well as a separate I/O range. Each register is described below. Unless otherwise indicated, bits are in the main (core) power well.

Bits not explicitly defined in each register are assumed to be reserved. When writing to a reserved bit, the value should always be 0. Software should not attempt to use the value read from a reserved bit, as it may not be consistently 1 or 0.

7.8.1 Power Management PCI Configuration Registers (PM—D31:F0)

Table 7-9 shows a small part of the configuration space for PCI Device 31: Function 0. It includes only those registers dedicated for power management. Some of the registers are only used for Legacy Power management schemes.

Table 7-9. Power Management PCI Register Address Map (PM—D31:F0) (Sheet 1 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
A0h–A1h	GEN_PMCON_1	General Power Management Configuration 1	0000h	R/W, R/WLO, RO
A2–A3h	GEN_PMCON_2	General Power Management Configuration 2	2000h	R/W, R/WC, RO
A4h–A5h	GEN_PMCON_3	General Power Management Configuration 3	4206h	R/W, R/WC, RO, R/WL

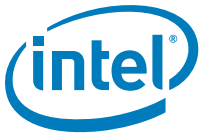


Table 7-9. Power Management PCI Register Address Map (PM—D31:F0) (Sheet 2 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
A6h	GEN_PMCON_LOCK	General Power Management Configuration Lock	00h	RO, R/WL
A9h	CIR4	Chipset Initialization Register 4	03h	R/W, RO
AAh	BM_BREAK_EN_2	BM_BREAK_EN Register #2	00h	R/W, RO
ABh	BM_BREAK_EN	BM_BREAK_EN Register	00h	R/W, RO
ACh–AFh	PMIR	Power Management Initialization	00000000h	R/W, R/WLO
B8h–BBh	GPI_ROUT	GPI Routing Control Register	00000000h	R/W
BCh–BFh	GPI_ROUT2	GPI Routing Control Register #2	00000000h	R/W

7.8.1.1 GEN_PMCON_1—General PM Configuration 1 Register (PM—D31:F0)

Offset Address: A0–A1h
Default Value: 0000h
Lockable: No
Attribute: R/W, RO, R/WLO
Size: 16 bits
Usage: ACPI, Legacy
Power Well: Core

Bit	Description
15	Reserved
14	**GEN_PMCON_1 Field 4** — R/W. BIOS may write to this field.
13	**GEN_PMCON_1 Field 3** — R/W. BIOS may write to this field.
12	**GEN_PMCON_1 Field 2** — R/W. BIOS may write to this field.
11	**GEN_PMCON_1 Field 1** — R/W. BIOS must program this field to 1b.
10	**BIOS_PCI_EXP_EN** — R/W. This bit acts as a global enable for the SCI associated with the PCI Express* ports. 0 = The various PCI Express ports and processor cannot cause the PCI_EXP_STS bit to go active. 1 = The various PCI Express ports and processor can cause the PCI_EXP_STS bit to go active.
9	**PWRBTN_LVL** — RO. This bit indicates the current state of the PWRBTN# signal. 0 = Low 1 = High
8:7	Reserved
6	**SMI_LOCK_GP22** — R/WLO. When this bit is set, writes to GPI_ROUT2[7:6], ALT_GPI_SMI_EN2[3], and GP_IO_SEL[22] will have no effect. Once the SMI_LOCK_GP22 bit is set, writes of 0 to SMI_LOCK_GP22 have no effect (that is, once set, this bit can only be cleared by PLTRST#).
5	**SMI_LOCK_GP6** — R/WLO. When this bit is set, writes to GPI_ROUT[13:12], ALT_GPI_SMI_EN[6] and GP_IO_SEL[6] will have no effect. Once the SMI_LOCK_GP6 bit is set, writes of 0 to SMI_LOCK_GP6 have no effect (that is, once set, this bit can only be cleared by PLTRST#).
4	**SMI_LOCK** — R/WLO. When this bit is set, writes to the GLB_SMI_EN bit (PMBASE + 30h, bit 0) will have no effect. Once the SMI_LOCK bit is set, writes of 0 to SMI_LOCK bit will have no effect (that is, once set, this bit can only be cleared by PLTRST#).
3	**Pseudo CLKRUN_EN(PSEUDO_CLKRUN_EN)** — R/W. 0 = Disable. 1 = Enable internal CLKRUN# logic to allow BDX PLL shutdown. This bit has no impact on state of external CLKRUN# pin. ***Notes:*** 1. PSEUDO_CLKRUN_EN bit does not result in STP_PCI# assertion to actually stop the external PCICLK. 2. This bit should be set mutually exclusive with the CLKRUN_EN bit.
2	Reserved

Bit	Description
1:0	**Periodic SMI# Rate Select (PER_SMI_SEL)** — R/W. Set by software to control the rate at which periodic SMI# is generated. 00 = 64 seconds 01 = 32 seconds 10 = 16 seconds 11 = 8 seconds

7.8.1.2 GEN_PMCON_2—General PM Configuration 2 Register (PM—D31:F0)

Offset Address:	A2–A3h	Attribute:	R/W, RO, R/WC
Default Value:	2000h	Size:	16 bits
Lockable:	No	Usage:	ACPI, Legacy
		Power Well:	RTC, SUS

Bit	Description
15:13	Reserved
12	AG3_PP_EN - R/W. After G3 PHY Power Enable. • When this bit is cleared (default), SLP_LAN# will be driven low upon exiting G3. • When this bit is set, SLP_LAN# value is dependent on DSX_PP_DIS and Sx_PP_EN setting. Refer to Section 3.12.9.4 for more details on SLP_LAN# value. This bit is reset by RTCRST#.
11	Sx_PP_EN - R/W. Sx PHY Power Enable (Non G3 to Sx entry) • When this bit is cleared (default), SLP_LAN# will be driven low in Sx/Moff. • When this bit is set, SLP_LAN# will be driven high in Sx/Moff. Refer to Section 3.12.9.4 for more details on SLP_LAN# value. This bit is on VccSUS3_3 and is reset when Suspend is reset.
10:8	Reserved
7	**DRAM Initialization Bit** — R/W. This bit does not affect hardware functionality in any way. BIOS is expected to set this bit prior to starting the DRAM initialization sequence and to clear this bit after completing the DRAM initialization sequence. BIOS can detect that a DRAM initialization sequence was interrupted by a reset by reading this bit during the boot sequence. • If the bit is 1, then the DRAM initialization was interrupted. • This bit is reset by the assertion of the RSMRST# pin.
6	Reserved
5	**Memory Placed in Self-Refresh (MEM_SR)** — RO. • If the bit is 1, DRAM should have remained powered and held in Self-Refresh through the last power state transition (that is, the last time the system left S0). • This bit is reset by the assertion of the RSMRST# pin.
4	**System Reset Status (SRS)** — R/WC. Software clears this bit by writing a 1 to it. 0 = SYS_RESET# button Not pressed. 1 = Intel® Xeon® Processor D-1500 Product Family sets this bit when the SYS_RESET# button is pressed. BIOS is expected to read this bit and clear it, if it is set. ***Notes:*** 1. This bit is also reset by RSMRST# and CF9h resets. 2. The SYS_RESET# is implemented in the Main power well. This pin must be properly isolated and masked to prevent incorrectly setting this Suspend well status bit.
3	**Processor Thermal Trip Status (CTS)** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = This bit is set when PLTRST# is inactive and THRMTRIP# goes active while the system is in an S0 or S1 state. ***Notes:*** 1. This bit is also reset by RSMRST#, and CF9h resets. It is not reset by the shutdown and reboot associated with the processor THRMTRIP# event. 2. The CF9h reset in the description refers to CF9h type core well reset which includes SYS_RESET#, PCH_PWROK/SYS_PWROK low, SMBus hard reset, TCO Timeout. This type of reset will clear CTS bit.

Bit	Description
2	**Minimum SLP_S4# Assertion Width Violation Status** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = Hardware sets this bit when the SLP_S4# assertion width is less than the time programmed in the SLP_S4# Minimum Assertion Width field (D31:F0:Offset A4h:bits 5:4). Intel® Xeon® Processor D-1500 Product Family begins the timer when SLP_S4# is asserted during S4/S5 entry or when the RSMRST# input is de-asserted during SUS well power-up. This bit is functional regardless of the values in the SLP_S4# Assertion Stretch Enable (D31:F0:Offset A4h:bit 3) and in the Disable SLP Stretching after SUS Well Power Up (D31:F0:Offset A4h:bit 12). ***Note:*** This bit is reset by the assertion of the RSMRST# pin, but can be set in some cases before the default value is readable.
1	**SYS_PWROK Failure (SYSPWR_FLR)** — R/WC. 0 = This bit will be cleared only be software writing a 1 back to the bit or by SUS well power loss. 1 = This bit will be set any time SYS_PWROK drops unexpectedly when the system was in S0 or S1 state.
0	**PWROK Failure (PWROK_FLR)** — R/WC. 0 = This bit will be cleared only be software writing a 1 back to the bit or by SUS well power loss. 1 = This bit will be set any time PWROK goes low when the system was in S0 or S1 state. ***Note:*** See Section 3.12.9.3 for more details about the PWROK pin functionality.

7.8.1.3 GEN_PMCON_3—General PM Configuration 3 Register (PM—D31:F0)

Offset Address:	A4-A5h	Attribute:	R/W, R/WC, RO, R/WL
Default Value:	4206h	Size:	16 bits
Lockable:	No	Usage:	ACPI, Legacy
		Power Well:	RTC, SUS

Bit	Description
15	**PME B0 S5 Disable (PME_B0_S5_DIS)**— R/W. When set to 1, this bit blocks wake events from PME_B0_STS in S5, regardless of the state of PME_B0_EN. When cleared (default), wake events from PME_B0_STS are allowed in S5 if PME_B0_EN = 1. Wakes from power states other than S5 are not affected by this policy bit. The net effect of setting PME_B0_S5_DIS = '1' is described by the truth table below: Y = Wake; N = Don't wake; B0 = PME_B0_EN; OV = WoL Enable Override **B0/OV** / **S1/S4** / **S5** 00 / N / N 01 / N / Y (LAN only) 11 / Y (all PME B0 sources) / Y (LAN only) 10 / Y (all PME B0 sources) / N This bit is cleared by the RTCRST# pin.
14	**SUS Well Power Failure (SUS_PWR_FLR)** — R/WC. 0 = Software writes a 1 to this bit to clear it. 1 = This bit is set to '1' whenever SUS well power is lost, as indicated by RSMRST# assertion. This bit is in the SUS well, and defaults to '1' based on RSMRST# assertion (not cleared by any type of reset).
13	**WoL Enable Override (WOL_EN_OVRD)** — R/W. 0 = WoL policies are determined by PMEB0 enable bit and appropriate LAN status bits 1 = Enable appropriately configured integrated LAN to wake the system in S5 only regardless of the value in the PME_B0_EN bit in the GPE0_EN register. This bit is cleared by the RTCRST# pin.

Bit	Description
12	**Disable SLP Stretching After SUS Well Power Up (DIS_SLP_STRCH_SUS_UP)**: R/WL 0 = Enables stretching on SLP signals after SUS power failure as enabled and configured in other fields. 1 = Disables stretching on SLP signals when powering up after a SUS well power loss. regardless of the state of the SLP_S4# Assertion Stretch Enable (bit 3). This bit is cleared by the RTCRST# pin. ***Notes:*** 1. This field is RO when the SLP Stretching Policy Lock-Down bit is set. 2. If this bit is cleared, SLP stretch timers start on SUS well power up (Intel® Xeon® Processor D-1500 Product Family has no ability to count stretch time while the SUS well is powered down). 3. This policy bit has a different effect on SLP_SUS# stretching than on the other SLP_* pins since SLP_SUS# is the control signal for one of the scenarios where SUS well power is lost the effect of setting this bit to '1' on: — SLP_S3# and SLP_S4# stretching: disabled after any SUS power loss. — SLP_SUS# stretching: disabled after G3,
11:10	**SLP_S3# Minimum Assertion Width (SLP_S3_MIN_ASST_WDTH):** R/WL This 2-bit value indicates the minimum assertion width of the SLP_S3# signal to ensure that the Main power supplies have been fully power-cycled. Valid Settings are: 00 = 60 us 01 = 1 ms 10 = 50 ms 11 = 2 s This bit is cleared by the RSMRST# pin. ***Note:*** This field is RO when the SLP Stretching Policy Lock-Down bit is set.
9	**General Reset Status** (GEN_RST_STS) — R/WC. This bit is set by hardware whenever PLTRST# asserts for any reason other than going into a software-entered sleep state (using PM1CNT.SLP_EN write) or a suspend well power failure (RSMRST# pin assertion). BIOS is expected to consult and then write a 1 to clear this bit during the boot flow before determining what action to take based on PM1_STS.WAK_STS = 1. If GEN_RST_STS = 1, the cold reset boot path should be followed rather than the resume path, regardless of the setting of WAK_STS. This bit is cleared by the RSMRST# pin.
8	Reserved.
7:6	**SWSMI_RATE_SEL** — R/W. This field indicates when the SWSMI timer will time out. Valid values are: 00 = 1.5 ms ± 0.6 ms 01 = 16 ms ± 4 ms 10 = 32 ms ± 4 ms 11 = 64 ms ± 4 ms These bits are not cleared by any type of reset except RTCRST#.

Bit	Description
5:4	**SLP_S4# Minimum Assertion Width(SLP_S4_MIN_ASST_WDTH)**— R/WL. This field indicates the minimum assertion width of the SLP_S4# signal to ensure that the DRAM modules have been safely power-cycled. Valid values are: 11 = 1 second 10 = 2 seconds 01 = 3 seconds 00 = 4 seconds This value is used in two ways: 1. If the SLP_S4# assertion width is ever shorter than this time, a status bit is set for BIOS to read when S0 is entered. 2. If enabled by bit 3 in this register, the hardware will prevent the SLP_S4# signal from de-asserting within this minimum time period after asserting. RTCRST# forces this field to the conservative default state (00b). ***Notes:*** 1. This field is RO when the SLP Stretching Policy Lock-Down bit is set. 2. The logic that measures this time is in the suspend power well. Therefore, when leaving a G3 state, the minimum time is measured from the de-assertion of the internal suspend well reset (unless the “Disable SLP Stretching After SUS Well Power Up” bit is set).
3	**SLP_S4# Assertion Stretch Enable** — R/WL. 0 = The SLP_S4# minimum assertion time is defined in Power Sequencing and Reset Signal Timings table. 1 = The SLP_S4# signal minimally assert for the time specified in bits 5:4 of this register. This bit is cleared by RTCRST#. ***Note:*** This bit is RO when the SLP Stretching Policy Lock-Down bit is set.
2	**RTC Power Status (RTC_PWR_STS)** — R/W. This bit is set when RTCRST# indicates a weak or missing battery. The bit is not cleared by any type of reset. The bit will remain set until the software clears it by writing a 0 back to this bit position.
1	**Power Failure (PWR_FLR)** — R/WC. This bit is in the DeepSx well and defaults to 1 based on DPWROK de-assertion (not cleared by any type of reset). 0 = Indicates that the trickle current has not failed since the last time the bit was cleared. Software clears this bit by writing a 1 to it. 1 = Indicates that the trickle current (from the main battery or trickle supply) was removed or failed. ***Note:*** Clearing CMOS in a Intel® Xeon® Processor D-1500 Product Family-based platform can be done by using a jumper on RTCRST# or GPI. Implementations should not attempt to clear CMOS by using a jumper to pull VccRTC low.
0	**AFTERG3_EN** — R/W. This bit determines what state to go to when power is re-applied after a power failure (G3 state). This bit is in the RTC well and is only cleared by RTCRST# assertion. 0 = System will return to S0 state (boot) after power is re-applied. 1 = System will return to the S5 state (except if it was in S4, in which case it will return to S4). In the S5 state, the only enabled wake event is the Power Button or any enabled wake event that was preserved through the power failure.

Note: RSMRST# is sampled using the RTC clock. Therefore, low times that are less than one RTC clock period may not be detected by Intel® Xeon® Processor D-1500 Product Family.

7.8.1.4 GEN_PMCON_LOCK—General Power Management Configuration Lock Register

Offset Address:	A6h	Attribute:	RO, R/WLO
Default Value:	00h	Size:	8 bits
Lockable:	No	Usage:	ACPI
Power Well:	Core		

Bit	Description
7:3	Reserved

Bit	Description
2	**SLP Stretching Policy Lock-Down (SLP_STR_POL_LOCK)** — R/WLO. When set to 1, this bit locks down the Disable SLP Stretching After SUS Well Power Up, SLP_S3# Minimum Assertion Width, SLP_S4# Minimum Assertion Width, SLP_S4# Assertion Stretch Enable bits in the GEN_PMCON_3 register, making them read-only. This bit becomes locked when a value of 1b is written to it. Writes of 0 to this bit are always ignored. This bit is cleared by platform reset.
1	**ACPI_BASE_LOCK** — R/WLO. When set to 1, this bit locks down the ACPI Base Address Register (ABASE) at offset 40h. The Base Address Field becomes read-only. This bit becomes locked when a value of 1b is written to it. Writes of 0 to this bit are always ignored. Once locked by writing 1, the only way to clear this bit is to perform a platform reset.
0	Reserved

7.8.1.5 CIR4—Chipset Initialization Register 4 (PM—D31:F0)

Offset Address:	A9h	Attribute:	R/W
Default Value:	03h	Size:	8 bits
Lockable:	No	Usage:	ACPI, Legacy
Power Well:	Core		

Bit	Description
7:0	**CIR4 Field 1** — R/W. BIOS may program this register.

7.8.1.6 BM_BREAK_EN_2 Register #2 (PM—D31:F0)

Offset Address:	AAh	Attribute:	R/W, RO
Default Value:	00h	Size:	8 bits
Lockable:	No	Usage:	ACPI, Legacy
Power Well:	Core		

Bit	Description
7:2	Reserved
1	**xHCI Break Enable (xHCI_BREAK_EN)** — R/W. 0 = xHCI traffic will not cause BM_STS to be set. 1 = xHCI traffic will cause BM_STS to be set.
0	**SATA3 Break Enable (SATA3_BREAK_EN)** — R/W. 0 = SATA3 traffic will not cause BM_STS to be set. 1 = SATA3 traffic will cause BM_STS to be set.

7.8.1.7 BM_BREAK_EN Register (PM—D31:F0)

Offset Address:	ABh	Attribute:	R/W, RO
Default Value:	00h	Size:	8 bits
Lockable:	No	Usage:	ACPI, Legacy
Power Well:	Core		

Bit	Description
7	**Storage Break Enable (STORAGE_BREAK_EN)** — R/W. 0 = Serial ATA traffic will not cause BM_STS to be set. 1 = Serial ATA traffic will cause BM_STS to be set.
6	**PCIE_BREAK_EN** — R/W. 0 = PCI Express* traffic will not cause BM_STS to be set. 1 = PCI Express traffic will cause BM_STS to be set.
5:3	Reserved
2	**EHCI_BREAK_EN** — R/W. 0 = EHCI traffic will not cause BM_STS to be set. 1 = EHCI traffic will cause BM_STS to be set.

Bit	Description
1:0	Reserved

7.8.1.8 GPI_ROUT—GPI Routing Control Register (PM—D31:F0)

Offset Address:	B8h–BBh	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits
Lockable:	No	Power Well:	Suspend

Bit	Description
31:30	**GPI 15 Route** — R/W. See bits 1:0 for description.
29:28	**GPI 14 Route** — R/W. See bits 1:0 for description.
27:26	**Reserved**
25:24	**GPI 12 Route** — R/W. See bits 1:0 for description.
23:22	**GPI 11 Route** — R/W. See bits 1:0 for description.
21:20	**GPI 10 Route** — R/W. See bits 1:0 for description.
19:18	**GPI 9 Route** — R/W. See bits 1:0 for description.
17:16	**GPI 8 Route** — R/W. See bits 1:0 for description.
15:14	**GPI 7 Route** — R/W. See bits 1:0 for description.
13:12	**GPI 6 Route** — R/W. See bits 1:0 for description.
11:10	**GPI 5 Route** — R/W. See bits 1:0 for description.
9:8	**GPI 4 Route** — R/W. See bits 1:0 for description.
7:6	**GPI 3 Route** — R/W. See bits 1:0 for description.
5:4	**GPI 2 Route** — R/W. See bits 1:0 for description.
3:2	**GPI 1 Route** — R/W. See bits 1:0 for description.
1:0	**GPI 0 Route** — R/W. If the corresponding GPIO is implemented and is configured as an Input, then a '1' in the corresponding GP_LVL bit can be routed to cause an interrupt. The type of interrupt (that is, NMI, SMI# or SCI) depends on the configuration bits in this register as well as the configuration bits in related registers, as described below. 00 = No effect. 01 = SMI# (if corresponding ALT_GPI_SMI_EN bit is also set). 10 = SCI (if corresponding GPE0_EN bit is also set). 11 = NMI (if corresponding GPI_NMI_EN is also set). If the system is in an S4–S5 state and if the GPE0_EN bit is also set, then the GPIO can cause a Wake event from Sx state, even if the GPIO is NOT routed to cause an NMI, SMI#, or SCI. Exception: If the system is in S5 state due to a power button override, then the GPIs will not cause wake events. Further, Core well GPIs are not capable of waking the system from sleep states where the Core well is not powered.

Note: If the GPIO is not set to an input, or if the Native function is selected, then the corresponding field in this register has no effect.

7.8.1.9 GPI_ROUT2—GPI Routing Control Register #2 (PM-D31:F0)

Offset Address:	BCh–BFh	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits
Lockable:	No	Power Well:	Suspend

Bit	Description
31:16	Reserved
15:14	**GPI60 Route** — R/W. See bits 1:0 for description.
13:12	**GPI57 Route** — R/W. See bits 1:0 for description.
11:10	**Reserved**
9:8	**GPI43 Route** — R/W. See bits 1:0 for description.
7:6	**GPI22 Route** — R/W. See bits 1:0 for description.
5:4	**GPI21 Route** — R/W. See bits 1:0 for description.
3:2	**GPI19 Route** — R/W. See bits 1:0 for description.
1:0	**GPI17 Route** — R/W. If the corresponding GPIO is implemented and is configured as an Input, then a '1' in the corresponding GP_LVL bit can be routed to cause an interrupt. The type of interrupt (that is, NMI, SMI# or SCI) depends on the configuration bits in this register as well as the configuration bits in related registers, as described below. 00 = No effect. 01 = SMI# (if corresponding ALT_GPI_SMI_EN2 bit is also set). 10 = SCI (if corresponding GPE0_EN bit is also set). 11 = NMI (if corresponding GPI_NMI_EN is also set). If the system is in an S4-S5 state and if the GPE0_EN bit is also set, then the GPIO can cause a Wake event from Sx state, even if the GPIO is NOT routed to cause an NMI, SMI# or SCI. Exception: If the system is in S5 state due to a power button override, then the GPIs will not cause wake events. Further, Core well GPIs are not capable of waking the system from sleep states where the Core well is not powered.

Note: If the GPIO is not set to an input, or if the Native function is selected, then the corresponding field in this register has no effect.

7.8.2 APM I/O Decode Register

Table 7-10 shows the I/O registers associated with APM support. This register space is enabled in the PCI Device 31: Function 0 space (APMDEC_EN), and cannot be moved (fixed I/O location).

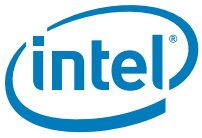
Table 7-10. APM Register Map

Address	Mnemonic	Register Name	Default	Type
B2h	APM_CNT	Advanced Power Management Control Port	00h	R/W
B3h	APM_STS	Advanced Power Management Status Port	00h	R/W

7.8.2.1 APM_CNT—Advanced Power Management Control Port Register

I/O Address:	B2h	Attribute:	R/W
Default Value:	00h	Size:	8 bits
Lockable:	No	Usage:	Legacy Only
Power Well:	Core		

Bit	Description
7:0	Used to pass an APM command between the OS and the SMI handler. Writes to this port not only store data in the APMC register, but also generates an SMI# when the APMC_EN bit is set.



7.8.2.2 APM_STS—Advanced Power Management Status Port Register

I/O Address:	B3h	Attribute:	R/W
Default Value:	00h	Size:	8 bits
Lockable:	No	Usage:	Legacy Only
Power Well:	Core		

Bit	Description
7:0	Used to pass data between the OS and the SMI handler. Basically, this is a scratchpad register and is not affected by any other register or function (other than a PCI reset).

7.8.3 Power Management I/O Registers

Table 7-11 shows the registers associated with ACPI and Legacy power management support. These registers locations are all offsets from the ACPI base address defined in the PCI Device 31: Function 0 space (PMBASE), and can be moved to any 128-byte aligned I/O location. In order to access these registers, the ACPI Enable bit (ACPI_EN) must be set. The registers are defined to support the ACPI 4.0a specification and generally use the same bit names.

Note: All reserved bits and registers will always return 0 when read, and will have no effect when written.

Table 7-11. ACPI and Legacy I/O Register Map

PMBASE + Offset	Mnemonic	Register Name	Default	Attribute
00h–01h	PM1_STS	PM1 Status	0000h	R/WC
02h–03h	PM1_EN	PM1 Enable	0000h	R/W
04h–07h	PM1_CNT	PM1 Control	00000000h	R/W, WO
08h–0Bh	PM1_TMR	PM1 Timer	00000000h	RO
20h–27h	GPE0_STS	General Purpose Event 0 Status	0000000000000000h	RO, R/WC
28h–2Fh	GPE0_EN	General Purpose Event 0 Enables	0000000000000000h	RO, R/W
30h–33h	SMI_EN	SMI# Control and Enable	00000002h	R/W, WO, R/WO
34h–37h	SMI_STS	SMI Status	00000000h	R/WC, RO
38h–39h	ALT_GPI_SMI_EN	Alternate GPI SMI Enable	0000h	R/W
3Ah–3Bh	ALT_GPI_SMI_STS	Alternate GPI SMI Status	0000h	R/WC
42h	GPE_CNTL	General Purpose Event Control	00h	R/W
44h–45h	DEVACT_STS	Device Activity Status	0000h	R/WC
50h	PM2_CNT	PM2 Control	00h	R/W
5Ch–5Dh	ALT_GPI_SMI_EN2	Alternate GPI SMI Enable 2 Register	0000h	R/W, RO
5Eh–5Fh	ALT_GPI_SMI_STS2	Alternate GPI SMI Status 2 Register	0000h	RO, RWC
60h–7Fh	—	Reserved for TCO	—	—

7.8.3.1 PM1_STS—Power Management 1 Status Register

I/O Address:	PMBASE + 00h	Attribute:	R/WC
Default Value:	0000h	Size:	16 bits
Lockable:	No	Usage:	ACPI or Legacy
Power Well:	Bits 0–7: Core, Bits 12-15: Suspend Bit 11: RTC, Bits 8, 10 and 14: Suspend		

If bit 10 or 8 in this register is set, and the corresponding _EN bit is set in the PM1_EN register, then Intel® Xeon® Processor D-1500 Product Family will generate a Wake Event. Once back in an S0 state (or if already in an S0 state when the event occurs), Intel® Xeon® Processor D-1500 Product Family will also generate an SCI if the SCI_EN bit is set, or an SMI# if the SCI_EN bit is not set.

Note: Bit 5 does not cause an SMI# or a wake event. Bit 0 does not cause a wake event but can cause an SMI# or SCI.

Bit	Description
15	**Wake Status (WAK_STS)** — R/WC. This bit is not affected by hard resets caused by a CF9 write, but is reset by RSMRST#. 0 = Software clears this bit by writing a 1 to it. 1 = Set by hardware when the system is in one of the sleep states (using the SLP_EN bit) and an enabled wake event occurs. Upon setting this bit, Intel® Xeon® Processor D-1500 Product Family will transition the system to the ON state. If the AFTERG3_EN bit is not set and a power failure (such as removed batteries) occurs without the SLP_EN bit set, the system will return to an S0 state when power returns, and the WAK_STS bit will not be set. If the AFTERG3_EN bit is set and a power failure occurs without the SLP_EN bit having been set, the system will go into an S5 state when power returns, and a subsequent wake event will cause the WAK_STS bit to be set. Any subsequent wake event would have to be caused by either a Power Button press, or an enabled wake event that was preserved through the power failure (enable bit in the RTC well).
14	**PCI Express* Wake Status (PCIEXPWAK_STS)** — R/WC. 0 = Software clears this bit by writing a 1 to it. If the WAKE# pin is still active during the write or the PME message received indication has not been cleared in the root port, then the bit will remain active (that is, all inputs to this bit are level-sensitive). 1 = This bit is set by hardware to indicate that the system woke due to a PCI Express wakeup event. This wakeup event can be caused by the PCI Express WAKE# pin being active or receipt of a PCI Express PME message at a root port. This bit is set only when one of these events causes the system to transition from a non-S0 system power state to the S0 system power state. This bit is set independent of the state of the PCIEXP_WAKE_DIS bit. ***Note:*** This bit does not itself cause a wake event or prevent entry to a sleeping state. Thus, if the bit is 1 and the system is put into a sleeping state, the system will not automatically wake.
13:12	Reserved
11	**Power Button Override Status (PWRBTNOR_STS)** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = This bit is set any time a Power Button Override occurs (that is, the power button is pressed for at least 4 consecutive seconds), due to the corresponding bit in the SMBus slave message, Intel ME Initiated Power Button Override, Intel ME Initiated Host Reset with Power down or due to an internal thermal sensor catastrophic condition. The power button override causes an unconditional transition to the S5 state. The BIOS or SCI handler clears this bit by writing a 1 to it. This bit is not affected by hard resets using CF9h writes, and is not reset by RSMRST#. Thus, this bit is preserved through power failures. If this bit is still asserted when the global SCI_EN is set, an SCI will be generated.
10	**RTC Status (RTC_STS)** — R/WC. This bit is not affected by hard resets caused by a CF9 write, but is reset by DPWROK. 0 = Software clears this bit by writing a 1 to it. 1 = Set by hardware when the RTC generates an alarm (assertion of the IRQ8# signal). Additionally if the RTC_EN bit (PMBASE + 02h, bit 10) is set, the setting of the RTC_STS bit will generate a wake event.
9	Reserved

Bit	Description
8	**Power Button Status (PWRBTN__STS)** — R/WC. This bit is not affected by hard resets caused by a CF9 write but is reset by DPWROK. 0 = If the PWRBTN# signal is held low for more than 4 seconds, the hardware clears the PWRBTN_STS bit, sets the PWRBTNOR_STS bit, and the system transitions to the S5 state with only PWRBTN# enabled as a wake event. This bit can be cleared by software by writing a one to the bit position. 1 = This bit is set by hardware when the PWRBTN# signal is asserted Low, independent of any other enable bit. In the S0 state, while PWRBTN_EN and PWRBTN_STS are both set, an SCI (or SMI# if SCI_EN is not set) will be generated. In any sleeping state S1–S5, while PWRBTN_EN (PMBASE + 02h, bit 8) and PWRBTN_STS are both set, a wake event is generated. ***Note:*** If the PWRBTN_STS bit is cleared by software while the PWRBTN# signal is sell asserted, this will not cause the PWRBN_STS bit to be set. The PWRBTN# signal must go inactive and active again to set the PWRBTN_STS bit.
7:6	Reserved
5	**Global Status (GBL _STS)** — R/WC. 0 = The SCI handler should then clear this bit by writing a 1 to the bit location. 1 = Set when an SCI is generated due to BIOS wanting the attention of the SCI handler. BIOS has a corresponding bit, BIOS_RLS, which will cause an SCI and set this bit.
4	**Bus Master Status (BM_STS)** — R/WC. This bit will not cause a wake event, SCI or SMI#. 0 = Software clears this bit by writing a 1 to it. 1 = Set by Intel® Xeon® Processor D-1500 Product Family when a Intel® Xeon® Processor D-1500 Product Family-visible bus master requests access to memory or the BMBUSY# signal is active.
3:1	Reserved
0	**Timer Overflow Status (TMROF_STS)** — R/WC. 0 = The SCI or SMI# handler clears this bit by writing a 1 to the bit location. 1 = This bit gets set any time bit 22 of the 24-bit timer goes high (bits are numbered from 0 to 23). This will occur every 2.3435 seconds. When the TMROF_EN bit (PMBASE + 02h, bit 0) is set, then the setting of the TMROF_STS bit will additionally generate an SCI or SMI# (depending on the SCI_EN).

7.8.3.2 PM1_EN—Power Management 1 Enable Register

I/O Address:	PMBASE + 02h	Attribute:	R/W
Default Value:	0000h	Size:	16 bits
Lockable:	No	Usage:	ACPI or Legacy
Power Well:	Bits 0–7: Core, Bits 8–9, 11–13, 15: Suspend, Bit 14: Suspend, Bit 10: RTC		

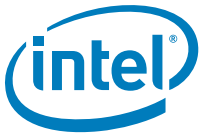
Bit	Description
15	Reserved
14	**PCI Express* Wake Disable(PCIEXPWAK_DIS)** — R/W. Modification of this bit has no impact on the value of the PCIEXP_WAKE_STS bit. 0 = Inputs to the PCIEXP_WAKE_STS bit in the PM1 Status register enabled to wake the system. 1 = Inputs to the PCIEXP_WAKE_STS bit in the PM1 Status register disabled from waking the system.
13:11	Reserved
10	**RTC Event Enable (RTC_EN)** — R/W. This bit is in the RTC well to allow an RTC event to wake after a power failure. 0 = No SCI (or SMI#) or wake event is generated then RTC_STS (PMBASE + 00h, bit 10) goes active. 1 = An SCI (or SMI#) or wake event will occur when this bit is set and the RTC_STS bit goes active.
9	Reserved

Bit	Description
8	**Power Button Enable (PWRBTN_EN)** — R/W. This bit is used to enable the setting of the PWRBTN_STS bit to generate a power management event (SMI#, SCI). PWRBTN_EN has no effect on the PWRBTN_STS bit (PMBASE + 00h, bit 8) being set by the assertion of the power button. The Power Button is always enabled as a Wake event. 0 = Disable. 1 = Enable.
7:6	Reserved
5	**Global Enable (GBL_EN)** — R/W. When both the GBL_EN and the GBL_STS bit (PMBASE + 00h, bit 5) are set, an SCI is raised. 0 = Disable. 1 = Enable SCI on GBL_STS going active.
4:1	Reserved
0	**Timer Overflow Interrupt Enable (TMROF_EN)** — R/W. Works in conjunction with the SCI_EN bit (PMBASE + 04h, bit 0) as described below: **TMROF_EN** / **SCI_EN** / **Effect when TMROF_STS is set** 0 / X / No SMI# or SCI 1 / 0 / SMI# 1 / 1 / SCI

7.8.3.3 PM1_CNT—Power Management 1 Control Register

I/O Address: PMBASE + 04h
Attribute: R/W, WO
Default Value: 00000000h
Size: 32 bits
Lockable: No
Usage: ACPI or Legacy
Power Well: Bits 0–9, 13-31: Core, Bits 10–12: RTC

Bit	Description
31:14	Reserved
13	**Sleep Enable** (**SLP_EN)** — WO. Setting this bit causes the system to sequence into the Sleep state defined by the SLP_TYP field.
12:10	**Sleep Type (SLP_TYP)** — R/W. This 3-bit field defines the type of Sleep the system should enter when the SLP_EN bit is set to 1. These bits are only reset by RTCRST#. **Code** / **Master Interrupt** 000b ON: Typically maps to S0 state. 001b Puts Processor Core in S1 state. 010b Reserved 011b Reserved 100b Reserved 101b Suspend-To-RAM. Assert SLP_S3#: Typically maps to S3 state. 110b Suspend-To-Disk. Assert SLP_S3#, and SLP_S4#: Typically maps to S4 state. 111b Soft Off. Assert SLP_S3#, SLP_S4#, and SLP_S5#: Typically maps to S5 state.
9:3	Reserved
2	**Global Release (GBL_RLS)** — WO. 0 = This bit always reads as 0. 1 = ACPI software writes a 1 to this bit to raise an event to the BIOS. BIOS software has a corresponding enable and status bits to control its ability to receive ACPI events.
1	**Bus Master Reload (BM_RLD)** — R/W. This bit is treated as a scratchpad bit. This bit is reset to 0 by PLTRST# 0 = Bus master requests will not cause a break from the C3 state. 1 = Enables Bus Master requests (internal or external) to cause a break from the C3 state. If software fails to set this bit before going to C3 state, Intel® Xeon® Processor D-1500 Product Family will still return to a snoopable state from C3 or C4 states due to bus master activity.



Bit	Description
0	**SCI Enable** (**SCI_EN**) — R/W. Selects the SCI interrupt or the SMI# interrupt for various events including the bits in the PM1_STS register (bit 10, 8, 0), and bits in GPE0_STS. 0 = These events will generate an SMI#. 1 = These events will generate an SCI.

7.8.3.4 PM1_TMR—Power Management 1 Timer Register

I/O Address:	PMBASE + 08h	Attribute:	RO
Default Value:	00000000h	Size:	32 bits
Lockable:	No	Usage:	ACPI
Power Well:	Core		

Bit	Description
31:24	Reserved
23:0	**Timer Value (TMR_VAL)** — RO. Returns the running count of the PM timer. This counter runs off a 3.579545 MHz clock (14.31818 MHz divided by 4). It is reset to 0 during a PCI reset, and then continues counting as long as the system is in the S0 state. After an S1 state, the counter will not be reset (it will continue counting from the last value in S0 state. Anytime bit 22 of the timer goes HIGH to LOW (bits referenced from 0 to 23), the TMROF_STS bit (PMBASE + 00h, bit 0) is set. The High-to-Low transition will occur every 2.3435 seconds. If the TMROF_EN bit (PMBASE + 02h, bit 0) is set, an SCI interrupt is also generated.

7.8.3.5 GPE0_STS—General Purpose Event 0 Status Register

I/O Address:	PMBASE + 20h	Attribute:	Bits 0:32,35 R/WC Bits 33:34, 36:63 RO
Default Value:	0000000000000000h	Size:	64-bit
Lockable:	No	Usage:	ACPI
Power Well:	Bits 0–34, 36-37, 56–63: Suspend, Bit 35, 38: Suspend		

This register is symmetrical to the General Purpose Event 0 Enable Register. Unless indicated otherwise below, if the corresponding _EN bit is set, then when the _STS bit get set, Intel® Xeon® Processor D-1500 Product Family will generate a Wake Event. Once back in an S0 state (or if already in an S0 state when the event occurs), Intel® Xeon® Processor D-1500 Product Family will also generate an SCI if the SCI_EN bit is set, or an SMI# if the SCI_EN bit (PMBASE + 04h, bit 0) is not set. Bits 31:16 are reset by a CF9h full reset; bits 63:32 and 15:0 are not. All bits (except bit 35) are reset by RSMRST#. Bit 35 is reset by DPWROK.

Bit	Description
63	**GPI60_STS - R/WC.** Refer to bit[56] in this register for description.
62	**GPI57_STS - R/WC.** Refer to bit[56] in this register for description.
61	**Reserved**
60	**GPI43_STS - R/WC.** Refer to bit[56] in this register for description.
59	**GPI22_STS - R/WC.** Refer to bit[56] in this register for description.
58	**GPI21_STS - R/WC.** Refer to bit[56] in this register for description.
57	**GPI19_STS - R/WC.** Refer to bit[56] in this register for description.
56	GPI17_STS — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = These bits are set any time the corresponding GPIO is set up as an input and the corresponding GPIO signal is high (or low if the corresponding GP_INV bit is set). If the corresponding enable bit is set in the GPE0_EN register, then when the GPI[n]_STS bit is set: • If the system is in an S1–S5 state, the event will also wake the system. • If the system is in an S0 state (or upon waking back to an S0 state), a SCI will be caused depending on the GPI_ROUT2 bits (D31:F0:BCh, bits 15:0) for the corresponding GPI.
55-39	Reserved

Bit	Description
38	Wake Alarm Device Timer Status (WADT_STS) — R/WC. This bit is set whenever any of the wake alarm device timers signal a timer expiration.
37:36	Reserved
35	**GPI27_STS** — R/WC. 0 = Disable. 1 = Set by hardware and can be reset by writing a one to this bit position or a resume well reset. This bit is set whenever GPIO27 is seen asserted low. GPIO27 is always monitored as an input for the purpose of setting this bit, regardless of the actual GPIO configuration.
34:32	Reserved
31:16	**GPIn_STS** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = These bits are set any time the corresponding GPIO is set up as an input and the corresponding GPIO signal is high (or low if the corresponding GP_INV bit is set). If the corresponding enable bit is set in the GPE0_EN register, then when the GPI[n]_STS bit is set: • If the system is in an S1–S5 state, the event will also wake the system. • If the system is in an S0 state (or upon waking back to an S0 state), a SCI will be caused depending on the GPI_ROUT bits (D31:F0:B8h, bits 31:30) for the corresponding GPI. ***Note:*** Mapping is as follows: bit 31 corresponds to GPI[15]... and bit 16 corresponds to GPI[0]. GPIO[13] is not supported.
15:14	Reserved
13	**PME_B0_STS** — R/WC. This bit will be set to 1 by Intel® Xeon® Processor D-1500 Product Family when any internal device with PCI Power Management capabilities on bus 0 asserts the equivalent of the PME# signal. Additionally, if the PME_B0_EN bit and SCI_EN bits are set, and the system is in an S0 state, then the setting of the PME_B0_STS bit will generate an SCI (or SMI# if SCI_EN is not set). If the PME_B0_EN bit is set, and the system is in an S1–S4 state (or S5 state due to SLP_TYP and SLP_EN), then the setting of the PME_B0_STS bit will generate a wake event. If the system is in an S5 state due to power button override, then the PME_B0_STS bit will not cause a wake event or SCI. The default for this bit is 0. Writing a 1 to this bit position clears this bit. The following are internal devices which can set this bit: • Intel Management Engine “maskable” wake events • Integrated LAN • SATA • EHCI
12	Reserved
11	**PME_STS** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = Set by hardware when the PME# signal goes active. Additionally, if the PME_EN and SCI_EN bits are set, and the system is in an S0 state, then the setting of the PME_STS bit will generate an SCI or SMI# (if SCI_EN is not set). If the PME_EN bit is set, and the system is in an S1–S4 state (or S5 state due to setting SLP_TYP and SLP_EN), then the setting of the PME_STS bit will generate a wake event. If the system is in an S5 state due to power button override or a power failure, then PME_STS will not cause a wake event or SCI.
10	Reserved

Bit	Description
9	**PCI_EXP_STS** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = Set by hardware to indicate that: — The PME event message was received on one or more of the PCI Express* ports — An Assert PMEGPE message received from the processor. ***Notes:*** 1. The PCI WAKE# pin has no impact on this bit. 2. If the PCI_EXP_STS bit went active due to an Assert PMEGPE message, then a Deassert PMEGPE message must be received prior to the software write in order for the bit to be cleared. 3. If the bit is not cleared and the corresponding PCI_EXP_EN bit is set, the level-triggered SCI will remain active. 4. A race condition exists where the PCI Express device sends another PME message because the PCI Express device was not serviced within the time when it must resend the message. This may result in a spurious interrupt, and this is comprehended and approved by the *PCI Express* Specification, Revision 1.0a*. The window for this race condition is approximately 95–105 milliseconds.
8	**RI_STS** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = Set by hardware when the RI# input signal goes active.
7	**SMBus Wake Status (SMB_WAK_STS)** — R/WC. Software clears this bit by writing a 1 to it. 0 = Wake event not caused by Intel® Xeon® Processor D-1500 Product Family's SMBus logic. 1 = Set by hardware to indicate that the wake event was caused by Intel® Xeon® Processor D-1500 Product Family's SMBus logic. The SMI handler should then clear this bit. **NOTES:** 1. The SMBus controller will independently cause an SMI# so this bit does not need to do so (unlike the other bits in this register). 2. This bit is set by the SMBus slave command 01h (Wake/SMI#) even when the system is in the S0 state. Therefore, to avoid an instant wake on subsequent transitions to sleep states, software must clear this bit after each reception of the Wake/SMI# command or just prior to entering the sleep state. 3. The SMBALERT_STS bit (SMB_BASE+00h:Bit 5) should be cleared by software before the SMB_WAK_STS bit is cleared.
6	**TCOSCI_STS** — R/WC. Software clears this bit by writing a 1 to it. 0 = TOC logic or thermal sensor logic did Not cause SCI. 1 = Set by hardware when the TCO logic or thermal sensor logic causes an SCI.
5:3	Reserved
2	**SWGPE_STS** — R/WC. The SWGPE_CTRL bit (bit 1 of GPE_CTRL reg) acts as a level input to this bit.
1	**HOT_PLUG_STS** — R/WC. 0 = This bit is cleared by writing a 1 to this bit position. 1 = When a PCI Express* Hot-Plug event occurs. This will cause an SCI if the HOT_PLUG_EN and SCI_EN bits are set.
0	Reserved

7.8.3.6 GPE0_EN—General Purpose Event 0 Enables Register

I/O Address:	PMBASE + 28h	Attribute:	R/W
Default Value:	0000000000000000h	Size:	64-bit
Lockable:	No	Usage:	ACPI
Power Well:	Bits 0–7, 9, 12, 14–34, 36–63 Suspend, Bits 8, 10–11, 13, 35 RTC		

This register is symmetrical to the General Purpose Event 0 Status Register.

Bit	Description
63	GPI[60]_EN - R/W. Refer to bit 56 for description.
62	GPI[57]_EN - R/W. Refer to bit 56 for description.
61	GPI[56]_EN - R/W. Refer to bit 56 for description.
60	GPI[43]_EN - R/W. Refer to bit 56 for description.
59	GPI[22]_EN - R/W. Refer to bit 56 for description.
58	GPI[21]_EN - R/W. Refer to bit 56 for description.
57	GPI[19]_EN - R/W. Refer to bit 56 for description.
56	GPI[17]_EN - R/W. This bit enables the corresponding GPI[n]_STS bits being set to cause an SCI and/or wake event.
55:39	Reserved
38	WADT_EN - R/W. Used to enable the setting of the WADT_STS bit to generate wake/SMI#/SCI.
37-36	Reserved
35	**GPI27_EN** — R/W. 0 = Disable. 1 = Enable the setting of the GPI27_STS bit to generate a wake event/SCI/SMI#. ***Note:*** Host wake events from the PHY through GPIO27 cannot be disabled by clearing this bit.
34:32	**Reserved**
31:16	**GPIn_EN** — R/W. These bits enable the corresponding GPI[n]_STS bits being set to cause a SCI, and/or wake event. These bits are cleared by RSMRST#. ***Note:*** Mapping is as follows: bit 31 corresponds to GPI15... and bit 16 corresponds to GPI0.
15:14	Reserved
13	**PME_B0_EN** — R/W. 0 = Disable ***Note:*** Enables the setting of the PME_B0_STS bit to generate a wake event and/or an SCI or SMI#.
12	Reserved
11	**PME_EN** — R/W. 0 = Disable. 1 = Enables the setting of the PME_STS to generate a wake event and/or an SCI. PME# can be a wake event from the S1–S4 state or from S5 (if entered using SLP_EN, but not power button override).
10	Reserved
9	**PCI_EXP_EN** — R/W. 0 = Disable SCI generation upon PCI_EXP_STS bit being set. 1 = Enables Intel® Xeon® Processor D-1500 Product Family to cause an SCI when PCI_EXP_STS bit is set. This is used to allow the PCI Express* ports, including the link to the processor, to cause an SCI due to wake/PME events.
8	**RI_EN** — R/W. The value of this bit will be maintained through a G3 state and is not affected by a hard reset caused by a CF9h write. 0 = Disable. 1 = Enables the setting of the RI_STS to generate a wake event.
7	Reserved
6	**TCOSCI_EN** — R/W. 0 = Disable. 1 = Enables the setting of the TCOSCI_STS to generate an SCI.
5:3	Reserved

Bit	Description
2	**SWGPE_EN**— R/W. This bit allows software to control the assertion of SWGPE_STS bit. This bit This bit, when set to 1, enables the SW GPE function. If SWGPE_CTRL is written to a 1, hardware will set SWGPE_STS (acts as a level input) If SWGPE_STS, SWGPE_EN, and SCI_EN are all 1s, an SCI will be generated If SWGPE_STS = 1, SWGPE_EN = 1, SCI_EN = 0, and GBL_SMI_EN = 1 then an SMI# will be generated
1	**HOT_PLUG_EN** — R/W. 0 = Disables SCI generation upon the HOT_PLUG_STS bit being set. 1 = Enables Intel® Xeon® Processor D-1500 Product Family to cause an SCI when the HOT_PLUG_STS bit is set. This is used to allow the PCI Express* ports to cause an SCI due to Hot-Plug events.
0	**Reserved**

7.8.3.7 SMI_EN—SMI Control and Enable Register

I/O Address:	PMBASE + 30h	Attribute:	R/W, R/WO, WO
Default Value:	00000002h	Size:	32 bit
Lockable:	No	Usage:	ACPI or Legacy
Power Well:	Core		

Note: This register is symmetrical to the SMI status register.

Bit	Description
31	**xHCI SMI Enable (xHCI _SMI_EN)** — R/W. 0 = Disable 1 = Enables xHCI to generate an SMI#
30	**ME SMI Enable (ME _SMI_EN)** — R/W. 0 = Disable 1 = Enables ME to generate an SMI#
29:28	Reserved
27	**GPIO_UNLOCK_SMI_EN**— R/WO. Setting this bit will cause Intel® Xeon® Processor D-1500 Product Family to generate an SMI# when the GPIO_UNLOCK_SMI_STS bit is set in the SMI_STS register. Once written to 1, this bit can only be cleared by PLTRST#.
26:19	Reserved
18	**INTEL_USB2_EN** — R/W. 0 = Disable 1 = Enables Intel-Specific EHCI SMI logic to cause SMI#.
17	**LEGACY_USB2_EN** — R/W. 0 = Disable 1 = Enables legacy EHCI logic to cause SMI#.
16:15	Reserved
14	**PERIODIC_EN** — R/W. 0 = Disable. 1 = Enables Intel® Xeon® Processor D-1500 Product Family to generate an SMI# when the PERIODIC_STS bit (PMBASE + 34h, bit 14) is set in the SMI_STS register (PMBASE + 34h).
13	**TCO_EN** — R/W. 0 = Disables TCO logic generating an SMI#. If the NMI2SMI_EN bit is set, SMIs that are caused by re-routed NMIs will not be gated by the TCO_EN bit. Even if the TCO_EN bit is 0, NMIs will still be routed to cause SMIs. 1 = Enables the TCO logic to generate SMI#. ***Note:*** This bit cannot be written once the TCO_LOCK bit is set.
12	Reserved
11	**MCSMI_EN Microcontroller SMI Enable (MCSMI_EN)** — R/W. 0 = Disable. 1 = Enables Intel® Xeon® Processor D-1500 Product Family to trap accesses to the microcontroller range (62h or 66h) and generate an SMI#. The "trapped' cycles will be claimed by Intel® Xeon® Processor D-1500 Product Family on PCI, but not forwarded to LPC.

Bit	Description
10:8	Reserved
7	**BIOS Release (BIOS_RLS)** — WO. 0 = This bit will always return 0 on reads. Writes of 0 to this bit have no effect. 1 = Enables the generation of an SCI interrupt for ACPI software when a one is written to this bit position by BIOS software. ***Note:*** GBL_STS being set will cause an SCI, even if the SCI_EN bit is not set. Software must take great care not to set the BIOS_RLS bit (which causes GBL_STS to be set) if the SCI handler is not in place.
6	**Software SMI# Timer Enable (SWSMI_TMR_EN)** — R/W. 0 = Disable. Clearing the SWSMI_TMR_EN bit before the timer expires will reset the timer and the SMI# will not be generated. 1 = Starts Software SMI# Timer. When the SWSMI timer expires (the timeout period depends upon the SWSMI_RATE_SEL bit setting), SWSMI_TMR_STS is set and an SMI# is generated. SWSMI_TMR_EN stays set until cleared by software.
5	**APMC_EN** — R/W. 0 = Disable. Writes to the APM_CNT register will not cause an SMI#. 1 = Enables writes to the APM_CNT register to cause an SMI#.
4	**SLP_SMI_EN** — R/W. 0 = Disables the generation of SMI# on SLP_EN. This bit must be 0 before the software attempts to transition the system into a sleep state by writing a 1 to the SLP_EN bit. 1 = A write of 1 to the SLP_EN bit (bit 13 in PM1_CNT register) will generate an SMI#, and the system will not transition to the sleep state based on that write to the SLP_EN bit.
3	**LEGACY_USB_EN** — R/W. 0 = Disable. 1 = Enables legacy USB circuit to cause SMI#.
2	**BIOS_EN** — R/W. 0 = Disable. 1 = Enables the generation of SMI# when ACPI software writes a 1 to the GBL_RLS bit (D31:F0:PMBase + 04h:bit 2). If the BIOS_STS bit (D31:F0:PMBase + 34h:bit 2), which gets set when software writes 1 to GBL_RLS bit, is already a 1 at the time that BIOS_EN becomes 1, an SMI# will be generated when BIOS_EN gets set.
1	**End of SMI (EOS)** — R/W (special). This bit controls the arbitration of the SMI signal to the processor. This bit must be set for Intel® Xeon® Processor D-1500 Product Family to assert SMI# low to the processor after SMI# has been asserted previously. 0 = Once Intel® Xeon® Processor D-1500 Product Family asserts SMI# low, the EOS bit is automatically cleared. 1 = When this bit is set to 1, SMI# signal will be de-asserted for 4 PCI clocks before its assertion. In the SMI handler, the processor should clear all pending SMIs (by servicing them and then clearing their respective status bits), set the EOS bit, and exit SMM. This will allow the SMI arbiter to re-assert SMI upon detection of an SMI event and the setting of a SMI status bit. ***Note:*** Intel® Xeon® Processor D-1500 Product Family is able to generate 1st SMI after reset even though EOS bit is not set. Subsequent SMI require EOS bit is set.
0	**GBL_SMI_EN** — R/W. 0 = No SMI# will be generated by Intel® Xeon® Processor D-1500 Product Family. This bit is reset by a PCI reset event. 1 = Enables the generation of SMI# in the system upon any enabled SMI event. ***Note:*** When the SMI_LOCK bit is set, this bit cannot be changed.

7.8.3.8 SMI_STS—SMI Status Register

I/O Address:	PMBASE + 34h	Attribute:	RO, R/WC
Default Value:	00000000h	Size:	32 bits
Lockable:	No	Usage:	ACPI or Legacy
Power Well:	Core		

Note: If the corresponding _EN bit is set when the _STS bit is set, Intel® Xeon® Processor D-1500 Product Family will cause an SMI# (except bits 8–10 and 12, which do not need enable bits since they are logic ORs of other registers that have enable bits). Intel® Xeon® Processor D-1500 Product Family uses the same GPE0_EN register (I/O address: PMBase+2Ch) to enable/disable both SMI and ACPI SCI general purpose input events. ACPI OS assumes that it owns the entire GPE0_EN register per the ACPI specification. Problems arise when some of the general-purpose inputs are enabled as

SMI by BIOS, and some of the general purpose inputs are enabled for SCI. In this case ACPI OS turns off the enabled bit for any GPIx input signals that are not indicated as SCI general-purpose events at boot, and exit from sleeping states. BIOS should define a dummy control method which prevents the ACPI OS from clearing the SMI GPE0_EN bits.

Bit	Description
31:28	Reserved
27	**GPIO_UNLOCK_SMI_STS** — R/WC. This bit will be set if the GPIO registers lockdown logic is requesting an SMI#. Writing a 1 to this bit position clears this bit to 0.
26	**SPI_STS** — RO. This bit will be set if the SPI logic is generating an SMI#. This bit is read only because the sticky status and enable bits associated with this function are located in the SPI registers.
25:22	Reserved
21	**MONITOR_STS** — RO. This bit will be set if the Trap/SMI logic has caused the SMI. This will occur when the processor or a bus master accesses an assigned register (or a sequence of accesses). See Section 5.1.16 through Section 5.1.32 for details on the specific cause of the SMI.
20	**PCI_EXP_SMI_STS** — RO. PCI Express* SMI event occurred. This could be due to a PCI Express* PME event or Hot-Plug event.
19	Reserved
18	**INTEL_USB2_STS** — RO. This non-sticky read-only bit is a logical OR of each of the SMI status bits in the Intel-Specific EHCI SMI Status Register ANDed with the corresponding enable bits. This bit will not be active if the enable bits are not set. Writes to this bit will have no effect. All integrated EHCIs are represented with this bit.
17	**LEGACY_USB2_STS** — RO. This non-sticky read-only bit is a logical OR of each of the SMI status bits in the EHCI Legacy Support Register ANDed with the corresponding enable bits. This bit will not be active if the enable bits are not set. Writes to this bit will have no effect. All integrated ECHIs are represented with this bit.
16	**SMBus SMI Status (SMBUS_SMI_STS)** — R/WC. Software clears this bit by writing a 1 to it. 0 = This bit is set from the 64 kHz clock domain used by the SMBus. Software must wait at least 15.63 µs after the initial assertion of this bit before clearing it. 1 = Indicates that the SMI# was caused by: 1. The SMBus Slave receiving a message that an SMI# should be caused, or 2. The SMBALERT# signal goes active and the SMB_SMI_EN bit is set and the SMBALERT_DIS bit is cleared, or 3. The SMBus Slave receiving a Host Notify message and the HOST_NOTIFY_INTREN and the SMB_SMI_EN bits are set, or 4. Intel® Xeon® Processor D-1500 Product Family detecting the SMLINK_SLAVE_SMI command while in the S0 state.
15	**SERIRQ_SMI_STS** — RO. 0 = SMI# was not caused by the SERIRQ decoder. 1 = Indicates that the SMI# was caused by the SERIRQ decoder. ***Note:*** This is not a sticky bit
14	**PERIODIC_STS** — R/WC. Software clears this bit by writing a 1 to it. 0 = Software clears this bit by writing a 1 to it. 1 = This bit is set at the rate determined by the PER_SMI_SEL bits. If the PERIODIC_EN bit (PMBASE + 30h, bit 14) is also set, Intel® Xeon® Processor D-1500 Product Family generates an SMI#.
13	**TCO_STS** — R/WC. Software clears this bit by writing a 1 to it. 0 = SMI# not caused by TCO logic. 1 = Indicates the SMI# was caused by the TCO logic. This is not a wake event.
12	**Device Monitor Status (DEVMON_STS)** — RO. 0 = SMI# not caused by Device Monitor. 1 = Set if bit 0 of the DEVACT_STS register (PMBASE + 44h) is set. The bit is not sticky, so writes to this bit will have no effect.
11	**Microcontroller SMI# Status** (**MCSMI_STS)** — R/WC. Software clears this bit by writing a 1 to it. 0 = Indicates that there has been no access to the power management microcontroller range (62h or 66h). 1 = Set if there has been an access to the power management microcontroller range (62h or 66h) and the Microcontroller Decode Enable #1 bit in the LPC Bridge I/O Enables configuration register is 1 (D31:F0:Offset 82h:bit 11). This implementation assumes that the Microcontroller is on LPC. If this bit is set, and the MCSMI_EN bit is also set, Intel® Xeon® Processor D-1500 Product Family will generate an SMI#.

Bit	Description
10	**GPE1_STS** — RO. This bit is a logical OR of the bits in the ALT_GPI_SMI_STS and the ALT_GPI_SMI_STS2 registers that are also set up to cause an SMI# (as indicated by the GPI_ROUT and GPI_ROUT2 registers) and have the corresponding bit set in the ALT_GPI_SMI_EN and ALT_GPI_SMI_EN2 registers. Bits that are not routed to cause an SMI# will have no effect on this bit. 0 = SMI# was not generated by a GPI assertion. 1 = SMI# was generated by a GPI assertion.
9	**GPE0_STS** — RO. This bit is a logical OR of the bits 35, 13, 11, 10, 8 and 2 in the GPE0_STS register (PMBASE + 28h) that also have the corresponding bit set in the GPE0_EN register (PMBASE + 2Ch). 0 = SMI# was not generated by a GPE0 event. 1 = SMI# was generated by a GPE0 event.
8	**PM1_STS_REG** — RO. This is an ORs of the bits in the ACPI PM1 Status Register (offset PMBASE+00h) that can cause an SMI#. 0 = SMI# was not generated by a PM1_STS event. 1 = SMI# was generated by a PM1_STS event.
7	Reserved
6	**SWSMI_TMR_STS** — R/WC. Software clears this bit by writing a 1 to it. 0 = Software SMI# Timer has Not expired. 1 = Set by the hardware when the Software SMI# Timer expires.
5	**APM_STS** — R/WC. Software clears this bit by writing a 1 to it. 0 = No SMI# generated by write access to APM Control register with APMCH_EN bit set. 1 = SMI# was generated by a write access to the APM Control register with the APMC_EN bit set.
4	**SLP_SMI_STS** — R/WC. Software clears this bit by writing a 1 to the bit location. 0 = No SMI# caused by write of 1 to SLP_EN bit when SLP_SMI_EN bit is also set. 1 = Indicates an SMI# was caused by a write of 1 to SLP_EN bit when SLP_SMI_EN bit is also set.
3	**LEGACY_USB_STS** — RO. This bit is a logical OR of each of the SMI status bits in the USB Legacy Keyboard/Mouse Control Registers ANDed with the corresponding enable bits. This bit will not be active if the enable bits are not set. 0 = SMI# was not generated by USB Legacy event. 1 = SMI# was generated by USB Legacy event.
2	**BIOS_STS** — R/WC. 0 = No SMI# generated due to ACPI software requesting attention. 1 = This bit gets set by hardware when a 1 is written by software to the GBL_RLS bit (D31:F0:PMBase + 04h:bit 2). When both the BIOS_EN bit (D31:F0:PMBase + 30h:bit 2) and the BIOS_STS bit are set, an SMI# will be generated. The BIOS_STS bit is cleared when software writes a 1 to its bit position.
1:0	Reserved

7.8.3.9 ALT_GPI_SMI_EN—Alternate GPI SMI Enable Register

I/O Address:	PMBASE +38h	Attribute:	R/W
Default Value:	0000h	Size:	16 bits
Lockable:	No	Usage:	ACPI or Legacy
Power Well:	Suspend		

Bit	Description
15:0	**Alternate GPI SMI Enable** — R/W. These bits are used to enable the corresponding GPIO to cause an SMI#. For these bits to have any effect, the following must be true. • The corresponding bit in the ALT_GPI_SMI_EN register is set. • The corresponding GPI must be routed in the GPI_ROUT register to cause an SMI. • The corresponding GPIO must be implemented. ***Note:*** Mapping is as follows: bit 15 corresponds to GPI15... bit 0 corresponds to GPI0. GPIO[13] is not supported.

7.8.3.10 ALT_GPI_SMI_STS—Alternate GPI SMI Status Register

I/O Address:	PMBASE +3Ah	Attribute:	R/WC
Default Value:	0000h	Size:	16 bits
Lockable:	No	Usage:	ACPI or Legacy
Power Well:	Suspend		

Bit	Description
15:0	**Alternate GPI SMI Status** — R/WC. These bits report the status of the corresponding GPIOs. 0 = Inactive. Software clears this bit by writing a 1 to it. 1 = Active These bits are sticky. If the following conditions are true, then an SMI# will be generated and the GPE0_STS bit set: • The corresponding bit in the ALT_GPI_SMI_EN register (PMBASE + 38h) is set • The corresponding GPIO must be routed in the GPI_ROUT register to cause an SMI. • The corresponding GPIO must be implemented. ***Note:*** All bits are in the resume well. Default for these bits is dependent on the state of the GPIO pins. GPIO[13] is not supported

7.8.3.11 GPE_CNTL—General Purpose Control Register

I/O Address:	PMBASE +42h	Attribute:	R/W
Default Value:	00h	Size:	8 bits
Lockable:	No	Usage:	ACPI or Legacy
Power Well:	Bits 0–1, 3–7: Suspend Bit 2: RTC		

Bit	Description
7:2	Reserved
1	**SWGPE_CTRL**— R/W. This bit allows software to control the assertion of SWGPE_STS bit. This bit is used by hardware as the level input signal for the SWGPE_STS bit in the GPE0_STS register. When SWGPE_CTRL is 1, SWGPE_STS will be set to 1, and writes to SWGPE_STS with a value of 1 to clear SWGPE_STS will result in SWGPE_STS being set back to 1 by hardware. When SWGPE_CTRL is 0, writes to SWGPE_STS with a value of 1 will clear SWGPE_STS to 0. In addition to being cleared by RSMRST# assertion, Intel® Xeon® Processor D-1500 Product Family also clears this bit due to a Power Button Override event, Intel ME Initiated Power Button Override, Intel ME Initiated Host Reset with Power down, SMBus unconditional power down, processor thermal trip event, or due to an internal thermal sensor catastrophic condition.
0	Reserved

7.8.3.12 DEVACT_STS—Device Activity Status Register

I/O Address:	PMBASE +44h	Attribute:	R/WC
Default Value:	0000h	Size:	16 bits
Lockable:	No	Usage:	Legacy Only
Power Well:	Core		

Each bit indicates if an access has occurred to the corresponding device's trap range, or for bits 6:9 if the corresponding PCI interrupt is active. This register is used in conjunction with the Periodic SMI# timer to detect any system activity for legacy power management. The periodic SMI# timer indicates if it is the right time to read the DEVACT_STS register (PMBASE + 44h).

Note: Software clears bits that are set in this register by writing a 1 to the bit position.

Bit	Description
15:13	Reserved
12	**KBC_ACT_STS** — R/WC. KBC (60/64h). 0 = Indicates that there has been no access to this device I/O range. 1 = This device I/O range has been accessed. Clear this bit by writing a 1 to the bit location.

Bit	Description
11:10	Reserved
9	**PIRQDH_ACT_STS — R/WC**. PIRQ[D or H]. 0 = The corresponding PCI interrupts have not been active. 1 = At least one of the corresponding PCI interrupts has been active. Clear this bit by writing a 1 to the bit location.
8	**PIRQCG_ACT_STS — R/WC**. PIRQ[C or G]. 0 = The corresponding PCI interrupts have not been active. 1 = At least one of the corresponding PCI interrupts has been active. Clear this bit by writing a 1 to the bit location.
7	**PIRQBF_ACT_STS — R/WC**. PIRQ[B or F]. 0 = The corresponding PCI interrupts have not been active. 1 = At least one of the corresponding PCI interrupts has been active. Clear this bit by writing a 1 to the bit location.
6	**PIRQAE_ACT_STS — R/WC**. PIRQ[A or E]. 0 = The corresponding PCI interrupts have not been active. 1 = At least one of the corresponding PCI interrupts has been active. Clear this bit by writing a 1 to the bit location.
5:0	Reserved

7.8.3.13 PM2_CNT—Power Management 2 Control Register

I/O Address:	PMBASE + 50h	Attribute:	R/W
Default Value:	00h	Size:	8 bits
Lockable:	No	Usage:	ACPI
Power Well:	Core		

Bit	Description
7:1	Reserved
0	**Arbiter Disable (ARB_DIS)** — R/W This bit is a scratchpad bit for legacy software compatibility.

7.8.3.14 ALT_GPI_SMI_EN2 - Alternate GPI SMI Enable 2 Register

I/O Address:	PMBASE + 5Ch	Attribute:	R/W, RO
Default Value:	0000h	Size:	16 bits
Lockable:	No	Usage:	ACPI
Power Well:	Suspend		

Bit	Description
15:8	Reserved
7	**Alternate GPI[60] SMI Enable (ALT_GPI60_SMI_EN) —** R/W. Refer to bit [0] in this register for description.
6	**Alternate GPI[57] SMI Enable (ALT_GPI57_SMI_EN) —** R/W. Refer to bit [0] in this register for description.
5	**Reserved**
4	**Alternate GPI[43] SMI Enable (ALT_GPI43_SMI_EN) —** R/W. Refer to bit [0] in this register for description.
3	**Alternate GPI[22] SMI Enable (ALT_GPI22_SMI_EN) —** R/W. Refer to bit [0] in this register for description.
2	**Alternate GPI[21] SMI Enable (ALT_GPI21_SMI_EN) —** R/W. Refer to bit [0] in this register for description.
1	**Alternate GPI[19] SMI Enable (ALT_GPI19_SMI_EN) —** R/W. Refer to bit [0] in this register for description.
0	**Alternate GPI[17] SMI Enable (ALT_GPI17_SMI_EN)** — R/W. These bits are used to enable the corresponding GPIO to cause an SMI#. For these bits to have any effect, the following must be true. • The corresponding bit in the ALT_GPI_SMI_STS2 register is set. • The corresponding GPI must be routed in the GPI_ROUT2 register to cause an SMI. • The corresponding GPIO must be implemented.

7.8.3.15 ALT_GPI_SMI_STS2—Alternate GPI SMI Status 2 Register

I/O Address:	PMBASE + 5E-5Fh	Attribute:	R/W, RO
Default Value:	00h	Size:	16 bits
Lockable:	No	Usage:	ACPI
Power Well:	Suspend		

Bit	Description
15:8	Reserved
7	**Alternate GPI[60] SMI Status (ALT_GPI60_SMI_STS) - R/W.** Refer to bit[0] in this register for description.
6	**Alternate GPI[57] SMI Status (ALT_GPI57_SMI_STS) - R/W.** Refer to bit[0] in this register for description.
5	**Reserved**
4	**Alternate GPI[43] SMI Status (ALT_GPI43_SMI_STS) - R/W.** Refer to bit[0] in this register for description.
3	**Alternate GPI[22] SMI Status (ALT_GPI22_SMI_STS) - R/W.** Refer to bit[0] in this register for description.
2	**Alternate GPI[21] SMI Status (ALT_GPI21_SMI_STS) - R/W.** Refer to bit[0] in this register for description.
1	**Alternate GPI[19] SMI Status (ALT_GPI19_SMI_STS) - R/W.** Refer to bit[0] in this register for description.
0	**Alternate GPI[17] SMI Status (ALT_GPI17_SMI_STS) - R/W.** These bits report the status of the corresponding GPIOs. 0 = Inactive. Software clears this bit by writing a 1 to it. 1 = Active These bits are sticky. If the following conditions are true, then an SMI# will be generated and the GPE0_STS bit set: • The corresponding bit in the ALT_GPI_SMI_EN2 register (PMBASE + 5Ch) is set • The corresponding GPIO must be routed in the GPI_ROUT2 register to cause an SMI. • The corresponding GPIO must be implemented.

7.9 System Management TCO Registers

The TCO logic is accessed using registers mapped to the PCI configuration space (D31:F0) and the system I/O space. For TCO PCI Configuration registers, see LPC D31:F0 PCI Configuration registers.

TCO Register I/O Map

The TCO I/O registers reside in a 32-byte range pointed to by a TCOBASE value, which is, PMBASE + 60h in the PCI config space. The following table shows the mapping of the registers within that 32-byte range. Each register is described in the following sections.

Table 7-12. TCO I/O Register Address Map (Sheet 1 of 2)

TCOBASE + Offset	Mnemonic	Register Name	Default	Attribute
00h–01h	TCO_RLD	TCO Timer Reload and Current Value	0000h	R/W
02h	TCO_DAT_IN	TCO Data In	00h	R/W
03h	TCO_DAT_OUT	TCO Data Out	00h	R/W
04h–05h	TCO1_STS	TCO1 Status	0000h	R/WC, RO
06h–07h	TCO2_STS	TCO2 Status	0000h	R/WC
08h–09h	TCO1_CNT	TCO1 Control	0000h	R/W, R/WLO, R/WC

Table 7-12. TCO I/O Register Address Map (Sheet 2 of 2)

TCOBASE + Offset	Mnemonic	Register Name	Default	Attribute
0Ah–0Bh	TCO2_CNT	TCO2 Control	0008h	R/W
0Ch–0Dh	TCO_MESSAGE1, TCO_MESSAGE2	TCO Message 1 and 2	00h	R/W
0Eh	TCO_WDCNT	TCO Watchdog Control	00h	R/W
0Fh	—	Reserved	—	—
10h	SW_IRQ_GEN	Software IRQ Generation	03h	R/W
11h	—	Reserved	—	—
12h–13h	TCO_TMR	TCO Timer Initial Value	0004h	R/W
14h–1Fh	—	Reserved	—	—

7.9.1 TCO_RLD—TCO Timer Reload and Current Value Register

I/O Address: TCOBASE +00h
Default Value: 0000h
Lockable: No
Attribute: R/W
Size: 16 bits
Power Well: Core

Bit	Description
15:10	Reserved
9:0	**TCO Timer Value** — R/W. Reading this register will return the current count of the TCO timer. Writing any value to this register will reload the timer to prevent the timeout.

7.9.2 TCO_DAT_IN—TCO Data In Register

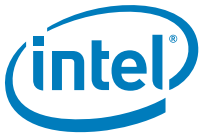
I/O Address: TCOBASE +02h
Default Value: 00h
Lockable: No
Attribute: R/W
Size: 8 bits
Power Well: Core

Bit	Description
7:0	**TCO Data In Value** — R/W. This data register field is used for passing commands from the OS to the SMI handler. Writes to this register will cause an SMI and set the SW_TCO_SMI bit in the TCO1_STS register (D31:F0:04h).

7.9.3 TCO_DAT_OUT—TCO Data Out Register

I/O Address: TCOBASE +03h
Default Value: 00h
Lockable: No
Attribute: R/W
Size: 8 bits
Power Well: Core

Bit	Description
7:0	**TCO Data Out Value** — R/W. This data register field is used for passing commands from the SMI handler to the OS. Writes to this register will set the TCO_INT_STS bit in the TCO1_STS register. It will also cause an interrupt, as selected by the TCO_INT_SEL bits.



7.9.4 TCO1_STS—TCO1 Status Register

I/O Address:	TCOBASE +04h	Attribute:	R/WC, RO
Default Value:	2000h	Size:	16 bits
Lockable:	No	Power Well:	Core (Except bit 7, in RTC)

Bit	Description
15:14	Reserved
13	**TCO_SLVSEL (TCO Slave Select)** — RO. This register bit is Read Only by Host and indicates the value of TCO Slave Select Soft Strap. Refer to Intel® Xeon® Processor D-1500 Product Family Soft Straps section of the SPI Chapter for details.
12	**BDXSERR_STS** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = Intel® Xeon® Processor D-1500 Product Family received a special cycle message indicating that it wants to cause an SERR#. The software must read the processor to determine the reason for the SERR#.
11	Reserved
10	**BDXSMI_STS** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = Intel® Xeon® Processor D-1500 Product Family received a special cycle message indicating that it wants to cause an SMI. The software must read the processor to determine the reason for the SMI.
9	**BDXSCI_STS** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = Intel® Xeon® Processor D-1500 Product Family received a special cycle message indicating that it wants to cause an SCI. The software must read to determine the reason for the SCI.
8	**BIOSWR_STS** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = Intel® Xeon® Processor D-1500 Product Family sets this bit and generates and SMI# to indicate an invalid attempt to write to the BIOS. This occurs when either: a) The BIOSWP bit is changed from 0 to 1 and the BLD bit is also set, or b) any write is attempted to the BIOS and the BIOSWP bit is also set. ***Note:*** On write cycles attempted to the 4 MB lower alias to the BIOS space, the BIOSWR_STS will not be set.
7	**NEWCENTURY_STS** — R/WC. This bit is in the RTC well. 0 = Cleared by writing a 1 to the bit position or by RTCRST# going active. 1 = This bit is set when the Year byte (RTC I/O space, index offset 09h) rolls over from 99 to 00. Setting this bit will cause an SMI# (but not a wake event). ***Note:*** The NEWCENTURY_STS bit is not valid when the RTC battery is first installed (or when RTC power has not been maintained). Software can determine if RTC power has not been maintained by checking the RTC_PWR_STS bit (D31:F0:A4h, bit 2), or by other means (such as a checksum on RTC RAM). If RTC power is determined to have not been maintained, BIOS should set the time to a valid value and then clear the NEWCENTURY_STS bit. The NEWCENTURY_STS bit may take up to 3 RTC clocks for the bit to be cleared after a 1 is written to the bit to clear it. After writing a 1 to this bit, software should not exit the SMI handler until verifying that the bit has actually been cleared. This will ensure that the SMI is not re-entered.
6:4	Reserved
3	**TIMEOUT** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = Set by Intel® Xeon® Processor D-1500 Product Family to indicate that the SMI was caused by the TCO timer reaching 0.
2	**TCO_INT_STS** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = SMI handler caused the interrupt by writing to the TCO_DAT_OUT register (TCOBASE + 03h).
1	**SW_TCO_SMI** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = Software caused an SMI# by writing to the TCO_DAT_IN register (TCOBASE + 02h).
0	**NMI2SMI_STS** — RO. 0 = Cleared by clearing the associated NMI status bit. 1 = Set by Intel® Xeon® Processor D-1500 Product Family when an SMI# occurs because an event occurred that would otherwise have caused an NMI (because NMI2SMI_EN is set).

7.9.5 TCO2_STS—TCO2 Status Register

I/O Address:	TCOBASE +06h	Attribute:	R/WC
Default Value:	0000h	Size:	16 bits
Lockable:	No	Power Well:	Resume (Except Bit 0, in RTC)

Bit	Description
15:5	Reserved
4	**SMLink Slave SMI Status (SMLINK_SLV_SMI_STS)** — R/WC. Allow the software to go directly into a pre-determined sleep state. This avoids race conditions. Software clears this bit by writing a 1 to it. 0 = The bit is reset by RSMRST#, but not due to the PCI Reset associated with exit from S4–S5 states. 1 = Intel® Xeon® Processor D-1500 Product Family sets this bit to 1 when it receives the SMI message on the SMLink Slave Interface.
3	Reserved
2	**BOOT_STS** — R/WC. 0 = Cleared by Intel® Xeon® Processor D-1500 Product Family based on RSMRST# or by software writing a 1 to this bit. Software should first clear the SECOND_TO_STS bit before writing a 1 to clear the BOOT_STS bit. 1 = Set to 1 when the SECOND_TO_STS bit goes from 0 to 1 and the processor has not fetched the first instruction. If rebooting due to a second TCO timer timeout, and if the BOOT_STS bit is set, Intel® Xeon® Processor D-1500 Product Family will reboot using the 'safe' multiplier (1111). This allows the system to recover from a processor frequency multiplier that is too high, and allows the BIOS to check the BOOT_STS bit at boot. If the bit is set and the frequency multiplier is 1111, then the BIOS knows that the processor has been programmed to an invalid multiplier.
1	**SECOND_TO_STS** — R/WC. 0 = Software clears this bit by writing a 1 to it, or by a RSMRST#. 1 = Intel® Xeon® Processor D-1500 Product Family sets this bit to 1 to indicate that the TIMEOUT bit had been (or is currently) set and a second timeout occurred before the TCO_RLD register was written. If this bit is set and the NO_REBOOT config bit is 0, then Intel® Xeon® Processor D-1500 Product Family will reboot the system after the second timeout. The reboot is done by asserting PLTRST#.
0	**Intruder Detect (INTRD_DET)** — R/WC. 0 = Software clears this bit by writing a 1 to it, or by RTCRST# assertion. 1 = Set by Intel® Xeon® Processor D-1500 Product Family to indicate that an intrusion was detected. This bit is set even if the system is in G3 state. ***Notes:*** 1. This bit has a recovery time. After writing a 1 to this bit position (to clear it), the bit may be read back as a 1 for up 65 microseconds before it is read as a 0. Software must be aware of this recovery time when reading this bit after clearing it. 2. If the INTRUDER# signal is active when the software attempts to clear the INTRD_DET bit, the bit will remain as a 1, and the SMI# will be generated again immediately. The SMI handler can clear the INTRD_SEL bits (TCOBASE + 0Ah, bits 2:1), to avoid further SMIs. However, if the INTRUDER# signals goes inactive and then active again, there will not be further SMI's (because the INTRD_SEL bits would select that no SMI# be generated). 3. If the INTRUDER# signal goes inactive some point after the INTRD_DET bit is written as a 1, then the INTRD_DET signal will go to a 0 when INTRUDER# input signal goes inactive. This is slightly different than a classic sticky bit, since most sticky bits would remain active indefinitely when the signal goes active and would immediately go inactive when a 1 is written to the bit.

7.9.6 TCO1_CNT—TCO1 Control Register

I/O Address:	TCOBASE +08h	Attribute:	R/W, R/WLO, R/WC
Default Value:	0000h	Size:	16 bits
Lockable:	No	Power Well:	Core

Bit	Description
15:13	Reserved
12	**TCO_LOCK** — R/WLO. When set to 1, this bit prevents writes from changing the TCO_EN bit (in offset 30h of Power Management I/O space). Once this bit is set to 1, it can not be cleared by software writing a 0 to this bit location. A core-well reset is required to change this bit from 1 to 0. This bit defaults to 0.
11	**TCO Timer Halt (TCO_TMR_HLT)** — R/W. 0 = The TCO Timer is enabled to count. 1 = The TCO Timer will halt. It will not count, and thus cannot reach a value that will cause an SMI# or set the SECOND_TO_STS bit. When set, this bit will prevent rebooting and prevent Alert On LAN event messages from being transmitted on the SMLink (but not Alert On LAN* heartbeat messages).
10	Reserved
9	**NMI2SMI_EN** — R/W. 0 = Normal NMI functionality. 1 = Forces all NMIs to instead cause SMIs. The functionality of this bit is dependent upon the settings of the NMI_EN bit and the GBL_SMI_EN bit as detailed in the following table: **NMI_EN** / **GBL_SMI_EN** / **Description** 0b / 0b / No SMI# at all because GBL_SMI_EN = 0 0b / 1b / SMI# will be caused due to NMI events 1b / 0b / No SMI# at all because GBL_SMI_EN = 0 1b / 1b / No SMI# due to NMI because NMI_EN = 1
8	**NMI_NOW** — R/WC. 0 = Software clears this bit by writing a 1 to it. The NMI handler is expected to clear this bit. Another NMI will not be generated until the bit is cleared. 1 = Writing a 1 to this bit causes an NMI. This allows the BIOS or SMI handler to force an entry to the NMI handler.
7:0	Reserved

7.9.7 TCO2_CNT—TCO2 Control Register

I/O Address:	TCOBASE +0Ah	Attribute:	R/W
Default Value:	0008h	Size:	16 bits
Lockable:	No	Power Well:	Resume

Bit	Description
15:6	Reserved
5:4	**OS_POLICY** — R/W. OS-based software writes to these bits to select the policy that the BIOS will use after the platform resets due the WDT. The following convention is recommended for the BIOS and OS: 00 = Boot normally 01 = Shut down 10 = Do not load OS. Hold in pre-boot state and use LAN to determine next step 11 = Reserved ***Note:*** These are just scratchpad bits. They should not be reset when the TCO logic resets the platform due to Watchdog Timer.
3	**GPIO11_ALERT_DISABLE** — R/W. At reset (using RSMRST# asserted) this bit is set and GPIO[11] alerts are disabled. 0 = Enable. 1 = Disable GPIO11/SMBALERT# as an alert source for the heartbeats and the SMBus slave.

Bit	Description
2:1	**INTRD_SEL** — R/W. This field selects the action to take if the INTRUDER# signal goes active. 00 = No interrupt or SMI# 01 = Interrupt (as selected by TCO_INT_SEL). 10 = SMI 11 = Reserved
0	Reserved

7.9.8 TCO_MESSAGE1 and TCO_MESSAGE2 Registers

I/O Address:	TCOBASE +0Ch (Message 1) TCOBASE +0Dh (Message 2)	Attribute:	R/W
Default Value:	00h	Size:	8 bits
Lockable:	No	Power Well:	Resume

Bit	Description
7:0	**TCO_MESSAGE[*n*]** — R/W. BIOS can write into these registers to indicate its boot progress. The external microcontroller can read these registers to monitor the boot progress.

7.9.9 TCO_WDCNT—TCO Watchdog Control Register

Offset Address:	TCOBASE + 0Eh	Attribute:	R/W
Default Value:	00h	Size:	8 bits
Power Well:	Resume		

Bit	Description
7:0	The BIOS or system management software can write into this register to indicate more details on the boot progress. The register will reset to 00h based on a RSMRST# (but not PLTRST#). The external microcontroller can read this register to monitor boot progress.

7.9.10 SW_IRQ_GEN—Software IRQ Generation Register

Offset Address:	TCOBASE + 10h	Attribute:	R/W
Default Value:	03h	Size:	8 bits
Power Well:	Core		

Bit	Description
7:2	Reserved
1	**IRQ12_CAUSE** — R/W. When software sets this bit to 1, IRQ12 will be asserted. When software sets this bit to 0, IRQ12 will be de-asserted.
0	**IRQ1_CAUSE** — R/W. When software sets this bit to 1, IRQ1 will be asserted. When software sets this bit to 0, IRQ1 will be de-asserted.

7.9.11 TCO_TMR—TCO Timer Initial Value Register

I/O Address:	TCOBASE +12h	Attribute:	R/W
Default Value:	0004h	Size:	16 bits
Lockable:	No	Power Well:	Core

Bit	Description
15:10	Reserved
9:0	**TCO Timer Initial Value** — R/W. Value that is loaded into the timer each time the TCO_RLD register is written. Values of 0000h or 0001h will be ignored and should not be attempted. The timer is clocked at approximately 0.6 seconds, and thus allows timeouts ranging from 1.2 second to 613.8 seconds. ***Note:*** The timer has an error of ±1 tick (0.6 S). The TCO Timer will only count down in the S0 state.

7.10 General Purpose I/O Registers

The control for the general purpose I/O signals is handled through a 128-byte I/O space. The base offset for this space is selected by the GPIOBASE register.

Table 7-13. Registers to Control GPIO Address Map (Sheet 1 of 2)

GPIOBASE + Offset	Mnemonic	Register Name	Default	Attribute
00h–03h	GPIO_USE_SEL	GPIO Use Select	B96BA1FFh	R/W
04h–07h	GP_IO_SEL	GPIO Input/Output Select	EEFF6EFFh	R/W
08h–0Bh	—	Reserved	0h	—
0Ch–0Fh	GP_LVL	GPIO Level for Input or Output	02FE0100h	R/W
10h–13h	—	Reserved	0h	—
14h–17h	—	Reserved	0h	—
18h–1Bh	GPO_BLINK	GPIO Blink Enable	00040000h	R/W
1Ch–1Fh	GP_SER_BLINK	GP Serial Blink	00000000h	R/W
20h–23h	GP_SB_CMDSTS	GP Serial Blink Command Status	00080000h	R/W
24h–27h	GP_SB_DATA	GP Serial Blink Data	00000000h	R/W
28h–29h	GPI_NMI_EN	GPI NMI Enable	0000h	R/W
2Ah–2Bh	GPI_NMI_STS	GPI NMI Status	0000h	R/WC
2Ch–2Fh	GPI_INV	GPIO Signal Invert	00000000h	R/W
30h–33h	GPIO_USE_SEL2	GPIO Use Select 2	020300FFh	R/W
34h–37h	GP_IO_SEL2	GPIO Input/Output Select 2	1F57FFF4h	R/W
38h–3Bh	GP_LVL2	GPIO Level for Input or Output 2	A4AA0007h	R/W
3Ch-3Dh	GPI_NMI_EN_2	GPI NMI Enable 2	00h	R/W, RO
3Eh-3Fh	GPI_NMI_STS_2	GPI NMI Status 2	00h	R/WC, R0
40h–43h	GPIO_USE_SEL3	GPIO Use Select 3	00000130h	R/W
44h–47h	GP_IO_SEL3	GPIO Input/Output Select 3	00000FF0h	R/W
48h–4Bh	GP_LVL3	GPIO Level for Input or Output 3	000000C0h	R/W
4Ch–4Fh	—	Reserved	—	—
50h-53h	GPI_NMI_EN_3	GPI NMI Enable 3	00000000h	R/W, RO
54h-57h	GPI_NMI_STS_3	GPI NMI Status 3	00000000h	R/WC, R0
57h–5Ah	—	Reserved	—	—
60h–63h	GP_RST_SEL1	GPIO Reset Select 1	01000000h	R/W

Table 7-13. Registers to Control GPIO Address Map (Sheet 2 of 2)

GPIOBASE + Offset	Mnemonic	Register Name	Default	Attribute
64h–67h	GP_RST_SEL2	GPIO Reset Select 2	00000000h	R/W
68h–6Bh	GP_RST_SEL3	GPIO Reset Select 3	00000000h	R/W
6Ch–7Fh	—	Reserved	—	—

7.10.1 GPIO_USE_SEL—GPIO Use Select Register

Offset Address: GPIOBASE + 00h
Attribute: R/W
Default Value: B96BA1FFh
Size: 32 bits
Lockable: Yes
Power Well: Core for 0:7, 16:23, Resume for 8:15, 24:31

Bit	Description
31:14	**GPIO_USE_SEL[31:14]** — R/W. Each bit in this register enables the corresponding GPIO (if it exists) to be used as a GPIO, rather than for the native function. 0 = Signal used as native function. 1 = Signal used as a GPIO. ***Notes:*** 1. The following bits are always 1 because they are always unmultiplexed: 8, 15, 24, 27, and 28. 2. After a full reset (RSMRST#) all multiplexed signals in the resume and core wells are configured as their default function. After only a PLTRST#, the GPIOs in the core well are configured as their default function. 3. When configured to GPIO mode, the multiplexing logic will present the inactive state to native logic that uses the pin as an input. 4. All GPIOs are reset to the default state by CF9h reset. Other resume well GPIOs' reset behavior can be programmed using GP_RST_SEL registers.
13	**Reserved**
12:0	**GPIO_USE_SEL[12:0]** — R/W. Each bit in this register enables the corresponding GPIO (if it exists) to be used as a GPIO, rather than for the native function. 0 = Signal used as native function. 1 = Signal used as a GPIO. ***Notes:*** 1. The following bits are always 1 because they are always unmultiplexed: 8, 15, 24, 27, and 28. 2. After a full reset (RSMRST#) all multiplexed signals in the resume and core wells are configured as their default function. After only a PLTRST#, the GPIOs in the core well are configured as their default function. 3. When configured to GPIO mode, the multiplexing logic will present the inactive state to native logic that uses the pin as an input. 4. All GPIOs are reset to the default state by CF9h reset. Other resume well GPIOs' reset behavior can be programmed using GP_RST_SEL registers.

7.10.2 GP_IO_SEL—GPIO Input/Output Select Register

Offset Address:	GPIOBASE +04h	Attribute:	R/W
Default Value:	EEFF6EFFh	Size:	32 bits
Lockable:	Yes	Power Well:	Core for 0:7, 16:23, Resume for 8:15, 24:31

Bit	Description
31:14	**GP_IO_SEL[31:14]** — R/W. When configured in native mode (GPIO_USE_SEL[n] is 0), writes to these bits have no effect. The value reported in this register is undefined when programmed as native mode. 0 = Output. The corresponding GPIO signal is an output. 1 = Input. The corresponding GPIO signal is an input.
13	**Reserved**
12:0	**GP_IO_SEL[12:0]** — R/W. When configured in native mode (GPIO_USE_SEL[n] is 0), writes to these bits have no effect. The value reported in this register is undefined when programmed as native mode. 0 = Output. The corresponding GPIO signal is an output. 1 = Input. The corresponding GPIO signal is an input.

7.10.3 GP_LVL—GPIO Level for Input or Output Register

Offset Address:	GPIOBASE +0Ch	Attribute:	R/W
Default Value:	02FE0100h	Size:	32 bits
Lockable:	Yes	Power Well:	Core for 0:7, 16:23, Resume for 8:15, 24:31

Bit	Description
31:14	**GP_LVL[31:14]**— R/W. These registers are implemented as dual read/write with dedicated storage each. Write value will be stored in the write register, while read is coming from the read register which will always reflect the value of the pin. If GPIO[n] is programmed to be an output (using the corresponding bit in the GP_IO_SEL register), then the corresponding GP_LVL[n] write register value will drive a high or low value on the output pin. 1 = high, 0 = low. When configured in native mode (GPIO_USE_SEL[n] is 0), writes to these bits are stored but have no effect to the pin value. The value reported in this register is undefined when programmed as native mode.
13	**Reserved**
12:0	**GP_LVL[12:0]**— R/W. These registers are implemented as dual read/write with dedicated storage each. Write value will be stored in the write register, while read is coming from the read register which will always reflect the value of the pin. If GPIO[n] is programmed to be an output (using the corresponding bit in the GP_IO_SEL register), then the corresponding GP_LVL[n] write register value will drive a high or low value on the output pin. 1 = high, 0 = low. When configured in native mode (GPIO_USE_SEL[n] is 0), writes to these bits are stored but have no effect to the pin value. The value reported in this register is undefined when programmed as native mode.

7.10.4 GPO_BLINK—GPO Blink Enable Register

Offset Address:	GPIOBASE +18h	Attribute:	R/W
Default Value:	00040000h	Size:	32 bits
Lockable:	No	Power Well:	Core for 0:7, 16:23, Resume for 8:15, 24:31

Bit	Description
31:14	**GP_BLINK[31:14]** — R/W. The setting of this bit has no effect if the corresponding GPIO signal is programmed as an input. 0 = The corresponding GPIO will function normally. 1 = If the corresponding GPIO is programmed as an output, the output signal will blink at a rate of approximately once per second. The high and low times have approximately 0.5 seconds each. The GP_LVL bit is not altered when this bit is set. The value of the corresponding GP_LVL bit remains unchanged during the blink process, and does not effect the blink in any way. The GP_LVL bit is not altered when programmed to blink. It will remain at its previous value. These bits correspond to GPIO in the Resume well. These bits revert to the default value based on RSMRST# or a write to the CF9h register (but not just on PLTRST#).
13	**Reserved**
12:0	**GP_BLINK[12:0]** — R/W. The setting of this bit has no effect if the corresponding GPIO signal is programmed as an input. 0 = The corresponding GPIO will function normally. 1 = If the corresponding GPIO is programmed as an output, the output signal will blink at a rate of approximately once per second. The high and low times have approximately 0.5 seconds each. The GP_LVL bit is not altered when this bit is set. The value of the corresponding GP_LVL bit remains unchanged during the blink process, and does not effect the blink in any way. The GP_LVL bit is not altered when programmed to blink. It will remain at its previous value. These bits correspond to GPIO in the Resume well. These bits revert to the default value based on RSMRST# or a write to the CF9h register (but not just on PLTRST#).

Note: GPIO18 will blink by default immediately after reset. This signal could be connected to an LED to indicate a failed boot (by programming BIOS to clear GP_BLINK18 after successful POST).

7.10.5 GP_SER_BLINK—GP Serial Blink Register

Offset Address:	GPIOBASE +1Ch	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits
Lockable:	No	Power Well:	Core for 0:7, 16:23, Resume for 8:15, 24:31

Bit	Description
31:14	**GP_SER_BLINK[31:14]** — R/W. The setting of this bit has no effect if the corresponding GPIO is programmed as an input or if the corresponding GPIO has the GPO_BLINK bit set. When set to a 0, the corresponding GPIO will function normally. When using serial blink, this bit should be set to a 1 while the corresponding GP_IO_SEL bit is set to 1. Setting the GP_IO_SEL bit to 0 after the GP_SER_BLINK bit ensures Intel® Xeon® Processor D-1500 Product Family will not drive a 1 on the pin as an output. When this corresponding bit is set to a 1 and the pin is configured to output mode, the serial blink capability is enabled. Intel® Xeon® Processor D-1500 Product Family will serialize messages through an open-drain buffer configuration. The value of the corresponding GP_LVL bit remains unchanged and does not impact the serial blink capability in any way. Writes to this register have no effect when the corresponding pin is configured in native mode and the read value returned is undefined.
13	**Reserved**

Bit	Description
12:0	**GP_SER_BLINK[12:0]** — R/W. The setting of this bit has no effect if the corresponding GPIO is programmed as an input or if the corresponding GPIO has the GPO_BLINK bit set. When set to a 0, the corresponding GPIO will function normally. When using serial blink, this bit should be set to a 1 while the corresponding GP_IO_SEL bit is set to 1. Setting the GP_IO_SEL bit to 0 after the GP_SER_BLINK bit ensures Intel® Xeon® Processor D-1500 Product Family will not drive a 1 on the pin as an output. When this corresponding bit is set to a 1 and the pin is configured to output mode, the serial blink capability is enabled. Intel® Xeon® Processor D-1500 Product Family will serialize messages through an open-drain buffer configuration. The value of the corresponding GP_LVL bit remains unchanged and does not impact the serial blink capability in any way. Writes to this register have no effect when the corresponding pin is configured in native mode and the read value returned is undefined.

7.10.6 GP_SB_CMDSTS—GP Serial Blink Command Status Register

Offset Address:	GPIOBASE +20h	Attribute:	R/W, RO
Default Value:	00080000h	Size:	32 bits
Lockable:	No	Power Well:	Core

Bit	Description
31:24	Reserved
23:22	**Data Length Select (DLS)** — R/W. This field determines the number of bytes to serialize on GPIO. 00 = Serialize bits 7:0 of GP_SB_DATA (1 byte) 01 = Serialize bits 15:0 of GP_SB_DATA (2 bytes) 10 = Undefined – Software must not write this value 11 = Serialize bits 31:0 of GP_SB_DATA (4 bytes) Software should not modify the value in this register unless the Busy bit is clear. Writes to this register have no effect when the corresponding pin is configured in native mode and the read value returned is undefined.
21:16	**Data Rate Select (DRS)** — R/W. This field selects the number of 120ns time intervals to count between Manchester data transitions. The default of 8h results in a 960 ns minimum time between transitions. A value of 0h in this register produces undefined behavior. Software should not modify the value in this register unless the Busy bit is clear.
15:9	Reserved
8	**Busy** — RO. This read-only status bit is the hardware indication that a serialization is in progress. Hardware sets this bit to 1 based on the Go bit being set. Hardware clears this bit when the Go bit is cleared by the hardware.
7:1	Reserved
0	**Go** — R/W. This bit is set to 1 by software to start the serialization process. Hardware clears the bit after the serialized data is sent. Writes of 0 to this register have no effect. Software should not write this bit to 1 unless the Busy status bit is cleared.

7.10.7 GP_SB_DATA—GP Serial Blink Data Register

Offset Address:	GPIOBASE +24h	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits
Lockable:	No	Power Well:	Core

Bit	Description
31:0	**GP_SB_DATA[31:0]** — R/W. This register contains the data serialized out. The number of bits shifted out are selected through the DLS field in the GP_SB_CMDSTS register. This register should not be modified by software when the Busy bit is set.

7.10.8 GPI_NMI_EN—GPI NMI Enable Register

Offset Address:	GPIOBASE +28h	Attribute:	R/W
Default Value:	00000h	Size:	16 bits
Lockable:	No	Power Well:	Core for 0:7 Resume for 8:15

Bit	Description
15:14	**GPI_NMI_EN[15:14]. GPI NMI Enable:** This bit only has effect if the corresponding GPIO is used as an input and its GPI_ROUT register is being programmed to NMI functionality. When set to 1, it used to allow active-low and active-high inputs (depends on inversion bit) to cause NMI.
13	**Reserved**
12:0	**GPI_NMI_EN[12:0]. GPI NMI Enable:** This bit only has effect if the corresponding GPIO is used as an input and its GPI_ROUT register is being programmed to NMI functionality. When set to 1, it used to allow active-low and active-high inputs (depends on inversion bit) to cause NMI.

7.10.9 GPI_NMI_STS—GPI NMI Status Register

Offset Address:	GPIOBASE +2Ah	Attribute:	R/WC
Default Value:	00000h	Size:	16 bits
Lockable:	Yes	Power Well:	Core for 0:7 Resume for 8:15

Bit	Description
15:14	**GPI_NMI_STS[15:14]. GPI NMI Status:** GPI_NMI_STS[15:0]. GPI NMI Status: This bit is set if the corresponding GPIO is used as an input, and its GPI_ROUT register is being programmed to NMI functionality and also GPI_NMI_EN bit is set when it detects either: 1) active-high edge when its corresponding GPI_INV is configured with value 0. 2) active-low edge when its corresponding GPI_INV is configured with value 1. ***Note:*** Writing value of 1 will clear the bit, while writing value of 0 have no effect.
13	**Reserved**
12:0	**GPI_NMI_STS[12:0]. GPI NMI Status:** GPI_NMI_STS[15:0]. GPI NMI Status: This bit is set if the corresponding GPIO is used as an input, and its GPI_ROUT register is being programmed to NMI functionality and also GPI_NMI_EN bit is set when it detects either: 1) active-high edge when its corresponding GPI_INV is configured with value 0. 2) active-low edge when its corresponding GPI_INV is configured with value 1. ***Note:*** Writing value of 1 will clear the bit, while writing value of 0 have no effect.

7.10.10 GPI_INV—GPIO Signal Invert Register

Offset Address:	GPIOBASE +2Ch	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits
Lockable:	No	Power Well:	Core for 17, 16, 7:0

Bit	Description
31:16	Reserved
15:14	**Input Inversion (GP_INV[n])** — R/W. This bit only has effect if the corresponding GPIO is used as an input and used by the GPE logic, where the polarity matters. When set to '1', then the GPI is inverted as it is sent to the GPE logic that is using it. This bit has no effect on the value that is reported in the GP_LVL register. These bits are used to allow both active-low and active-high inputs to cause SMI# or SCI. In the S0 or S1 state, the input signal must be active for at least two PCI clocks to ensure detection by Intel® Xeon® Processor D-1500 Product Family. In the S4, or S5 states the input signal must be active for at least 2 RTC clocks to ensure detection. The setting of these bits has no effect if the corresponding GPIO is programmed as an output. These bits correspond to GPI that are in the resume well, and will be reset to their default values by RSMRST# or by a write to the CF9h register. 0 = The corresponding GPI_STS bit is set when Intel® Xeon® Processor D-1500 Product Family detects the state of the input pin to be high. 1 = The corresponding GPI_STS bit is set when Intel® Xeon® Processor D-1500 Product Family detects the state of the input pin to be low.
13	**Reserved**
12:0	**Input Inversion (GP_INV[n])** — R/W. This bit only has effect if the corresponding GPIO is used as an input and used by the GPE logic, where the polarity matters. When set to '1', then the GPI is inverted as it is sent to the GPE logic that is using it. This bit has no effect on the value that is reported in the GP_LVL register. These bits are used to allow both active-low and active-high inputs to cause SMI# or SCI. In the S0 or S1 state, the input signal must be active for at least two PCI clocks to ensure detection by Intel® Xeon® Processor D-1500 Product Family. In the S4, or S5 states the input signal must be active for at least 2 RTC clocks to ensure detection. The setting of these bits has no effect if the corresponding GPIO is programmed as an output. These bits correspond to GPI that are in the resume well, and will be reset to their default values by RSMRST# or by a write to the CF9h register. 0 = The corresponding GPI_STS bit is set when Intel® Xeon® Processor D-1500 Product Family detects the state of the input pin to be high. 1 = The corresponding GPI_STS bit is set when Intel® Xeon® Processor D-1500 Product Family detects the state of the input pin to be low.

7.10.11 GPIO_USE_SEL2—GPIO Use Select 2 Register

Offset Address:	GPIOBASE +30h	Attribute:	R/W
Default Value:	020300FFh	Size:	32 bits
Lockable:	Yes	Power Well:	Core for 0:7, 16:23, Resume for 8:15, 24:31

This register corresponds to GPIO[63:32].

Bit	Description
31:0	**GPIO_USE_SEL2[63:32]**— R/W. Each bit in this register enables the corresponding GPIO (if it exists) to be used as a GPIO, rather than for the native function. 0 = Signal used as native function. 1 = Signal used as a GPIO. ***Notes:*** 1. The following bits are always 1 because they are always unmultiplexed: 3, 25. The following bit is unmultiplexed and is also 1: 0. 2. If GPIO[n] does not exist, then, the (n-32) bit in this register will always read as 0 and writes will have no effect. 3. After a full reset RSMRST# all multiplexed signals in the resume and core wells are configured as their default function. After only a PLTRST#, the GPIOs in the core well are configured as their default function. 4. When configured to GPIO mode, the multiplexing logic will present the inactive state to native logic that uses the pin as an input. 5. Bit 26 is ignored, functionality is configured by bits 9:8 of FLMAP0 register.

7.10.12 GP_IO_SEL2—GPIO Input/Output Select 2 Register

Offset Address:	GPIOBASE +34h	Attribute:	R/W
Default Value:	1F57FFF4h		
Lockable:	Yes	Power Well:	Core for 0:7, 16:23, Resume for 8:15, 24:31

This register corresponds to GPIO[63:32].

Bit	Description
31:0	**GP_IO_SEL2[63:32]** — R/W. 0 = GPIO signal is programmed as an output. 1 = Corresponding GPIO signal (if enabled in the GPIO_USE_SEL2 register) is programmed as an input. ***Notes:*** If GPIO[n] does not exist, then, the (n-32) bit in this register will always read as 0 and writes will have no effect.

7.10.13 GP_LVL2—GPIO Level for Input or Output 2 Register

Offset Address:	GPIOBASE +38h	Attribute:	R/W
Default Value:	A4AA0007h	Size:	32 bits
Lockable:	Yes	Power Well:	Core for 0:7, 16:23, Resume for 8:15, 24:31

This register corresponds to GPIO[63:32].

Bit	Description
31:0	**GP_LVL[63:32]** — R/W. These registers are implemented as dual read/write with dedicated storage each. Write value will be stored in the write register, while read is coming from the read register which will always reflect the value of the pin. If GPIO[n] is programmed to be an output (using the corresponding bit in the GP_IO_SEL register), then the corresponding GP_LVL[n] write register value will drive a high or low value on the output pin. 1 = high, 0 = low. When configured in native mode (GPIO_USE_SEL[n] is 0), writes to these bits are stored but have no effect to the pin value. The value reported in this register is undefined when programmed as native mode. ***Notes:*** If GPIO[n] does not exist, then, the (n-32) bit in this register will always read as 0 and writes will have no effect.

7.10.14 GPI_NMI_EN_2—GPI NMI Enable Register 2

Offset Address:	GPIOBASE +3Ch	Attribute:	R/W, RO
Default Value:	00h	Size:	8 bits
Lockable:	No	Power Well:	Core for 0:7

Bit	Description
7:0	**GPI_NMI_EN[23:16]. GPI NMI Enable:** This bit only has effect if the corresponding GPIO is used as an input and its GPI_ROUT register is being programmed to NMI functionality. When set to 1, it used to allow active-low and active-high inputs (depends on inversion bit) to cause NMI. ***Note:*** Only bits 6, 5, 3, 1 (GPI_NMI_EN 22, 21, 19, 17) are implemented with Read/Write attribute. The remaining bits are RO of '0'. ***Note:*** Note that bit 1 in this register corresponds to GPI_NMI_EN[17].

7.10.15 GPI_NMI_STS_2—GPI NMI Status Register 2

Offset Address:	GPIOBASE +3Eh	Attribute:	R/WC, RO
Default Value:	00h	Size:	8 bits
Lockable:	Yes	Power Well:	Core for 0:7

Bit	Description
7:0	**GPI_NMI_STS[23:16]. GPI NMI Status:** GPI_NMI_STS[7:0]. GPI NMI Status: This bit is set if the corresponding GPIO is used as an input, and its GPI_ROUT register is being programmed to NMI functionality and also GPI_NMI_EN bit is set when it detects either: 1) active-high edge when its corresponding GPI_INV is configured with value 0. 2) active-low edge when its corresponding GPI_INV is configured with value 1. ***Note:*** Writing value of 1 will clear the bit, while writing value of 0 have no effect. ***Note:*** Only bits 6, 5, 3, 1 (GPI_NMI_EN 22, 21, 19, 17) are implemented with Read/Write Clear attribute. The remaining bits are RO of '0'.

7.10.16 GPIO_USE_SEL3—GPIO Use Select 3 Register

Offset Address:	GPIOBASE +40h	Attribute:	R/W
Default Value:	00000130h	Size:	32 bits
Lockable:	Yes	Power Well:	Core for 0:7, 16:23, Resume for 8:15, 24:31

This register corresponds to GPIO[75:64]. Bit 0 corresponds to GPIO64 and bit 11 corresponds to GPIO75.

Bit	Description
31:12	Always 0. No corresponding GPIO.
11:0	**GPIO_USE_SEL3[75:64]**— R/W. Each bit in this register enables the corresponding GPIO (if it exists) to be used as a GPIO, rather than for the native function. 0 = Signal used as native function. 1 = Signal used as a GPIO. ***Notes:*** 1. The following bit is always 1 because it is always unmultiplexed: 8 2. If GPIO[n] does not exist, then, the (n-64) bit in this register will always read as 0 and writes will have no effect. 3. After a full reset RSMRST# all multiplexed signals in the resume and core wells are configured as their default function. After only a PLTRST#, the GPIOs in the core well are configured as their default function. 4. When configured to GPIO mode, the multiplexing logic will present the inactive state to native logic that uses the pin as an input.

7.10.17 GP_IO_SEL3—GPIO Input/Output Select 3 Register

Offset Address:	GPIOBASE +44h	Attribute:	R/W
Default Value:	00000FF0h	Size:	32 bits
Lockable:	Yes	Power Well:	Core for 0:7, 16:23, Resume for 8:15, 24:31

This register corresponds to GPIO[75:64]. Bit 0 corresponds to GPIO64 and bit 11 corresponds to GPIO75.

Bit	Description
31:12	Always 0. No corresponding GPIO.
11:0	**GP_IO_SEL3[75:64]**— R/W. 0 = GPIO signal is programmed as an output. 1 = Corresponding GPIO signal (if enabled in the GPIO_USE_SEL3 register) is programmed as an input. ***Notes:*** If GPIO[n] does not exist, then, the (n-64) bit in this register will always read as 0 and writes will have no effect.

7.10.18 GP_LVL3—GPIO Level for Input or Output 3 Register

Offset Address:	GPIOBASE +48h	Attribute:	R/W
Default Value:	000000C0h	Size:	32 bits
Lockable:	Yes	Power Well:	Core for 0:7, 16:23, Resume for 8:15, 24:31

This register corresponds to GPIO[75:64]. Bit 0 corresponds to GPIO64 and bit 11 corresponds to GPIO75.

Bit	Description
31:12	Always 0. No corresponding GPIO.
11:0	**GP_LVL[75:64]** — R/W. These registers are implemented as dual read/write with dedicated storage each. Write value will be stored in the write register, while read is coming from the read register which will always reflect the value of the pin. If GPIO[n] is programmed to be an output (using the corresponding bit in the GP_IO_SEL register), then the corresponding GP_LVL[n] write register value will drive a high or low value on the output pin. 1 = high, 0 = low. When configured in native mode (GPIO_USE_SEL[n] is 0), writes to these bits are stored but have no effect to the pin value. The value reported in this register is undefined when programmed as native mode. ***Notes:*** If GPIO[n] does not exist, then, the (n-64) bit in this register will always read as 0 and writes will have no effect.

7.10.19 GPI_NMI_EN_3—GPI NMI Enable Register 3

Offset Address:	GPIOBASE +50h	Attribute:	R/W, RO
Default Value:	00000000h	Size:	32 bits
Lockable:	Yes	Power Well:	Core for 0:7, 16:23 Resume for 8:15, 24:31

Bit	Description
31:0	**GPI_NMI_EN[63:32]. GPI NMI Enable:** This bit only has effect if the corresponding GPIO is used as an input and its GPI_ROUT register is being programmed to NMI functionality. When set to 1, it used to allow active-low and active-high inputs (depends on inversion bit) to cause NMI. ***Note:*** Only bits 28, 25:24, 11(GPI_NMI_EN 60, 57, 56, 43) are implemented with Read/Write attribute. The remaining bits are RO of '0'. ***Note:*** Note that bit 31 in this register corresponds to GPI_NMI_EN[63].

7.10.20 GPI_NMI_STS_3—GPI NMI Status Register 3

Offset Address:	GPIOBASE +54	Attribute:	R/WC, RO
Default Value:	00000000h	Size:	32 bits
Lockable:	Yes	Power Well:	Core for 0:7, 16:23 Resume for 8:15, 24:31

Bit	Description
31:0	**GPI_NMI_STS[63:32]. GPI NMI Status:** GPI_NMI_STS[7:0]. GPI NMI Status: This bit is set if the corresponding GPIO is used as an input, and its GPI_ROUT register is being programmed to NMI functionality and also GPI_NMI_EN bit is set when it detects either: 1) active-high edge when its corresponding GPI_INV is configured with value 0. 2) active-low edge when its corresponding GPI_INV is configured with value 1. ***Note:*** Only bits 28, 25:24, 11(GPI_NMI_EN 60, 57, 56, 43) are implemented with Read/Write attribute. The remaining bits are RO of '0'. ***Note:*** Note that bit 31 in this register corresponds to GPI_NMI_EN[63].

7.10.21 GP_RST_SEL1 — GPIO Reset Select Register

Offset Address:	GPIOBASE +60h	Attribute:	R/W
Default Value:	01000000h	Size:	32 bits
Lockable:	Yes	Power Well:	Core for 0:7, 16:23, Resume for 8:15, 24:31

Bit	Description
31:24	**GP_RST_SEL[31:24]** — R/W. 0 = Corresponding GPIO registers will be reset by PWROK de-assertion, CF9h reset (06h or 0Eh), or SYS_RESET# assertion. 1 = Corresponding GPIO registers will be reset by RSMRST# assertion only. ***Note:*** GPIO[24] register bits are not cleared by CF9h reset by default.
23:16	Reserved
15:14	**GP_RST_SEL[15:14]** — R/W. 0 = Corresponding GPIO registers will be reset by PWROK de-assertion, CF9h reset (06h or 0Eh), or SYS_RESET# assertion. 1 = Corresponding GPIO registers will be reset by RSMRST# assertion only.
13	Reserved
12:8	**GP_RST_SEL[12:8]** — R/W. 0 = Corresponding GPIO registers will be reset by PWROK de-assertion, CF9h reset (06h or 0Eh), or SYS_RESET# assertion. 1 = Corresponding GPIO registers will be reset by RSMRST# assertion only.
7:0	Reserved

7.10.22 GP_RST_SEL2—GPIO Reset Select Register

Offset Address:	GPIOBASE +64h	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits
Lockable:	Yes	Power Well:	Core for 0:7, 16:23, Resume for 8:15, 24:31

Bit	Description
31	Reserved
30:25	**GP_RST_SEL[62:57]** — R/W. 0 = Corresponding GPIO registers will be reset by PWROK de-assertion, CF9h reset (06h or 0Eh), or SYS_RESET# assertion. 1 = Corresponding GPIO registers will be reset by RSMRST# assertion only.
24:15	Reserved
14:8	**GP_RST_SEL[46:40]** — R/W. 0 = Corresponding GPIO registers will be reset by PWROK de-assertion, CF9h reset (06h or 0Eh), or SYS_RESET# assertion. 1 = Corresponding GPIO registers will be reset by RSMRST# assertion only.
7:0	Reserved

7.10.23 GP_RST_SEL3—GPIO Reset Select Register

Offset Address:	GPIOBASE +68h	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits
Lockable:	Yes	Power Well:	Core for 0:7, 16:23, Resume for 8:15, 24:31

Bit	Description
31:12	Reserved
11:10	**GP_RST_SEL[75:74]** — R/W. 0 = Corresponding GPIO registers will be reset by PWROK de-assertion, CF9h reset (06h or 0Eh), or SYS_RESET# assertion. 1 = Corresponding GPIO registers will be reset by RSMRST# assertion only.
9	Reserved
8	**GP_RST_SEL[72]** — R/W. 0 = Corresponding GPIO registers will be reset by PWROK de-assertion, CF9h reset (06h or 0Eh), or SYS_RESET# assertion. 1 = Corresponding GPIO registers will be reset by RSMRST# assertion only.
7:0	Reserved

§

8 SATA Controller Registers (D31:F2)

8.1 PCI Configuration Registers (SATA–D31:F2)

Note: Address locations that are not shown should be treated as Reserved.

All of the SATA registers are in the core well. None of the registers can be locked.

Table 8-1. SATA Controller PCI Register Address Map (SATA–D31:F2) (Sheet 1 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
00h–01h	VID	Vendor Identification	8086h	RO
02h–03h	DID	Device Identification	See register description	RO
04h–05h	PCICMD	PCI Command	0000h	R/W, RO
06h–07h	PCISTS	PCI Status	02B0h	R/WC, RO
08h	RID	Revision Identification	See register description	RO
09h	PI	Programming Interface	See register description	See register description
0Ah	SCC	Sub Class Code	See register description	See register description
0Bh	BCC	Base Class Code	01h	RO
0Dh	PMLT	Primary Master Latency Timer	00h	RO
0Eh	HTYPE	Header Type	00h	RO
10h–13h	PCMD_BAR	Primary Command Block Base Address	00000001h	R/W, RO
14h–17h	PCNL_BAR	Primary Control Block Base Address	00000001h	R/W, RO
18h–1Bh	SCMD_BAR	Secondary Command Block Base Address	00000001h	R/W, RO
1Ch–1Fh	SCNL_BAR	Secondary Control Block Base Address	00000001h	R/W, RO
20h–23h	BAR	Legacy Bus Master Base Address	00000001h	R/W, RO
24h–27h	ABAR / SIDPBA	AHCI Base Address / SATA Index Data Pair Base Address	See register description	See register description
2Ch–2Dh	SVID	Subsystem Vendor Identification	0000h	R/WO
2Eh–2Fh	SID	Subsystem Identification	0000h	R/WO
34h	CAP	Capabilities Pointer	80h	RO
3Ch	INT_LN	Interrupt Line	00h	R/W
3Dh	INT_PN	Interrupt Pin	See register description	RO
40h–41h	IDE_TIM	Primary IDE Timing	0000h	R/W
42h–43h	IDE_TIM	Secondary IDE Timing	0000h	R/W
44h	SIDETIM	Slave IDE Timing	00h	R/W
48h	SDMA_CNT	Synchronous DMA Control	00h	R/W
4Ah–4Bh	SDMA_TIM	Synchronous DMA Timing	0000h	R/W
54h–57h	IDE_CONFIG	IDE I/O Configuration	00000000h	R/W
70h–71h	PID	PCI Power Management Capability Identification	See register description	RO

Table 8-1. SATA Controller PCI Register Address Map (SATA–D31:F2) (Sheet 2 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
72h–73h	PC	PCI Power Management Capabilities	See register description	RO
74h–75h	PMCS	PCI Power Management Control and Status	See register description	R/W, RO, R/WC
80h–81h	MSICI	Message Signaled Interrupt Capability Identification	7005h	RO
82h–83h	MSIMC	Message Signaled Interrupt Message Control	0000h	RO, R/W
84h–87h	MSIMA	Message Signaled Interrupt Message Address	00000000h	RO, R/W
88h–89h	MSIMD	Message Signaled Interrupt Message Data	0000h	R/W
90h	MAP	Address Map	0000h	R/W, R/WO
92h–93h	PCS	Port Control and Status	0000h	R/W, RO
94h–97h	SCLKCG	SATA Clock Gating Control	00000000h	R/W
9Ch–9Fh	SGC	SATA General Configuration	00000000h	R/W, R/WO
A8h–ABh	SATACR0	SATA Capability Register 0	0010B012h	RO, R/WO
ACh–AFh	SATACR1	SATA Capability Register 1	00000048h	RO
B0h–B1h	FLRCID	FLR Capability Identification	0009h	RO
B2h–B3h	FLRCLV	FLR Capability Length and Version	See register description	R/WO, RO
B4h–B5h	FLRC	FLR Control	0000h	RO, R/W
C0h	ATC	APM Trapping Control	00h	R/W
C4h	ATS	APM Trapping Status	00h	R/WC
D0h–D3h	SP	Scratch Pad	00000000h	R/W
E0h–E3h	BFCS	BIST FIS Control/Status	00000000h	R/W, R/WC
E4h–E7h	BFTD1	BIST FIS Transmit Data, DW1	00000000h	R/W
E8h–EBh	BFTD2	BIST FIS Transmit Data, DW2	00000000h	R/W

Note: Intel® Xeon® Processor D-1500 Product Family SATA controller is not arbitrated as a PCI device; therefore, it does not need a master latency timer.

8.1.1 VID—Vendor Identification Register (SATA—D31:F2)

Offset Address: 00h–01h
Default Value: 8086h
Lockable: No
Attribute: RO
Size: 16 bit
Power Well: Core

Bit	Description
15:0	**Vendor ID** — RO. This is a 16-bit value assigned to Intel. Intel VID = 8086h

8.1.2 DID—Device Identification Register (SATA—D31:F2)

Offset Address: 02h–03h
Default Value: See bit description
Lockable: No
Attribute: RO
Size: 16 bit
Power Well: Core

Bit	Description
15:0	**Device ID** — RO. This is a 16-bit value assigned to Intel® Xeon® Processor D-1500 Product Family SATA controller. ***Note:*** The value of this field will change dependent upon the value of the MAP Register. See Section 8.1.34

8.1.3 PCICMD—PCI Command Register (SATA–D31:F2)

Address Offset: 04h–05h
Default Value: 0000h
Attribute: RO, R/W
Size: 16 bits

Bit	Description
15:11	Reserved
10	**Interrupt Disable** — R/W. This disables pin-based INTx# interrupts. This bit has no effect on MSI operation. 0 = Internal INTx# messages are generated if there is an interrupt and MSI is not enabled. 1 = Internal INTx# messages will not be generated.
9	**Fast Back to Back Enable (FBE)** — RO. Hardwired to 0.
8	**SERR# Enable (SERR_EN)** — RO. Hardwired to 0.
7	**Wait Cycle Control (WCC)** — RO. Hardwired to 0.
6	**Parity Error Response (PER)** — R/W. 0 = Disabled. SATA controller will not generate PERR# when a data parity error is detected. 1 = Enabled. SATA controller will generate PERR# when a data parity error is detected.
5	**VGA Palette Snoop (VPS)** — RO. Hardwired to 0.
4	**Postable Memory Write Enable (PMWE)** — RO. Hardwired to 0.
3	**Special Cycle Enable (SCE)** — RO. Hardwired to 0.
2	**Bus Master Enable (BME)** — R/W. This bit controls the SATA controller's ability to act as a master for data transfers. This bit does not impact the generation of completions for split transaction commands.
1	**Memory Space Enable (MSE)** — R/W / RO. Controls access to the SATA controller's target memory space (for AHCI). This bit is RO 0 when not in AHCI/RAID modes.
0	**I/O Space Enable (IOSE)** — R/W. This bit controls access to the I/O space registers. 0 = Disables access to the Legacy or Native IDE ports (both Primary and Secondary) as well as the Bus Master I/O registers. 1 = Enable. The Base Address register for the Bus Master registers should be programmed before this bit is set.

8.1.4 PCISTS — PCI Status Register (SATA–D31:F2)

Address Offset: 06h–07h
Default Value: 02B0h
Attribute: R/WC, RO
Size: 16 bits

Note: For the writable bits, software must write a 1 to clear bits that are set. Writing a 0 to the bit has no effect.

Bit	Description
15	**Detected Parity Error (DPE)** — R/WC. 0 = No parity error detected by SATA controller. 1 = SATA controller detects a parity error on its interface.
14	**Signaled System Error (SSE)** — RO. Hardwired to 0.
13	**Received Master Abort (RMA)** — R/WC. 0 = Master abort not generated. 1 = SATA controller, as a master, generated a master abort.
12	Reserved — R/WC.
11	**Signaled Target Abort (STA)** — RO. Hardwired to 0.
10:9	**DEVSEL# Timing Status (DEV_STS)** — RO. 01 = Hardwired; Controls the device select time for the SATA controller's PCI interface.
8	**Data Parity Error Detected (DPED)** — R/WC. For Intel® Xeon® Processor D-1500 Product Family, this bit can only be set on read completions received from the bus when there is a parity error. 0 = No data parity error received. 1 = SATA controller, as a master, either detects a parity error or sees the parity error line asserted, and the parity error response bit (bit 6 of the command register) is set.
7	**Fast Back to Back Capable (FB2BC)** — RO. Hardwired to 1.
6	Reserved

Bit	Description
5	**66MHz Capable (66MHZ_CAP)** — RO. Hardwired to 1.
4	**Capabilities List (CAP_LIST)** — RO. This bit indicates the presence of a capabilities list. The minimum requirement for the capabilities list must be PCI power management for the SATA controller.
3	**Interrupt Status (INTS)** — RO. Reflects the state of INTx# messages, IRQ14 or IRQ15. 0 = Interrupt is cleared (independent of the state of Interrupt Disable bit in the command register [offset 04h]). 1 = Interrupt is to be asserted
2:0	Reserved

8.1.5 RID—Revision Identification Register (SATA—D31:F2)

Offset Address: 08h Attribute: RO
Default Value: See bit description Size: 8 bits

Bit	Description
7:0	**Revision ID** — RO. This field indicates the device specific revision identifier.

8.1.6 PI—Programming Interface Register (SATA–D31:F2)

8.1.6.1 When Sub Class Code Register (D31:F2:Offset 0Ah) = 01h

Address Offset: 09h Attribute: R/W, RO
Default Value: 8Ah Size: 8 bits

Bit	Description
7	Reserved. This read-only bit is a 1 to indicate that Intel® Xeon® Processor D-1500 Product Family supports bus master operation
6:4	Reserved. Will always return 0.
3	**Secondary Mode Native Capable (SNC)** — RO. Hardwired to '1' to indicate secondary controller supports both legacy and native modes.
2	**Secondary Mode Native Enable (SNE)** — R/W. Determines the mode that the secondary channel is operating in. 0 = Secondary controller operating in legacy (compatibility) mode 1 = Secondary controller operating in native PCI mode. If this bit is set by software, then the PNE bit (bit 0 of this register) must also be set by software. While in theory these bits can be programmed separately, such a configuration is not supported by hardware.
1	**Primary Mode Native Capable (PNC)** — RO. Hardwired to '1' to indicate primary controller supports both legacy and native modes.
0	**Primary Mode Native Enable (PNE)** — R/W. Determines the mode that the primary channel is operating in. 0 = Primary controller operating in legacy (compatibility) mode. 1 = Primary controller operating in native PCI mode. If this bit is set by software, then the SNE bit (bit 2 of this register) must also be set by software simultaneously.

8.1.6.2 When Sub Class Code Register (D31:F2:Offset 0Ah) = 04h

Address Offset: 09h Attribute: RO
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Interface (IF)** — RO. When configured as RAID, this register becomes read only 0.

8.1.6.3 When Sub Class Code Register (D31:F2:Offset 0Ah) = 06h

Address Offset: 09h Attribute: RO
Default Value: 01h Size: 8 bits

Bit	Description
7:0	**Interface (IF)** — RO. Indicates that the SATA Controller is an AHCI HBA that has a major revision of 1.

8.1.7 SCC—Sub Class Code Register (SATA–D31:F2)

Address Offset: 0Ah Attribute: RO
Default Value: See bit description Size: 8 bits

Bit	Description
7:0	**Sub Class Code (SCC)** This field specifies the sub-class code of the controller, per the table below: **MAP.SMS (D31:F2:Offset 90h:bit 7:6) Value** — **SCC Register Value** 00b — 01h (IDE Controller) 01b — 06h (AHCI Controller) 10b — 04h (RAID Controller)

8.1.8 BCC—Base Class Code Register (SATA–D31:F2SATA–D31:F2)

Address Offset: 0Bh Attribute: RO
Default Value: 01h Size: 8 bits

Bit	Description
7:0	**Base Class Code (BCC)** — RO. 01h = Mass storage device

8.1.9 PMLT—Primary Master Latency Timer Register (SATA–D31:F2)

Address Offset: 0Dh Attribute: RO
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Master Latency Timer Count (MLTC)** — RO. 00h = Hardwired. The SATA controller is implemented internally, and is not arbitrated as a PCI device, so it does not need a Master Latency Timer.

8.1.10 HTYPE—Header Type Register (SATA–D31:F2)

Address Offset: 0Eh Attribute: RO
Default Value: 00h Size: 8 bits

Bit	Description
7	**Multi-function Device (MFD)** — RO. Indicates this SATA controller is not part of a multifunction device.
6:0	**Header Layout (HL)** — RO. Indicates that the SATA controller uses a target device layout.

8.1.11 PCMD_BAR—Primary Command Block Base Address Register (SATA–D31:F2)

Address Offset: 10h–13h
Attribute: R/W, RO
Default Value: 00000001h
Size: 32 bits

Bit	Description
31:16	Reserved
15:3	**Base Address** — R/W. This field provides the base address of the I/O space (8 consecutive I/O locations).
2:1	Reserved
0	**Resource Type Indicator (RTE)** — RO. Hardwired to 1 to indicate a request for I/O space.

Note: This 8-byte I/O space is used in native mode for the Primary Controller's Command Block.

8.1.12 PCNL_BAR—Primary Control Block Base Address Register (SATA–D31:F2)

Address Offset: 14h–17h
Attribute: R/W, RO
Default Value: 00000001h
Size: 32 bits

Bit	Description
31:16	Reserved
15:2	**Base Address** — R/W. This field provides the base address of the I/O space (4 consecutive I/O locations).
1	Reserved
0	**Resource Type Indicator (RTE)** — RO. Hardwired to 1 to indicate a request for I/O space.

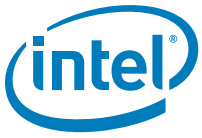
Note: This 4-byte I/O space is used in native mode for the Primary Controller's Control Block.

8.1.13 SCMD_BAR—Secondary Command Block Base Address Register (SATA D31:F2)

Address Offset: 18h–1Bh
Attribute: R/W, RO
Default Value: 00000001h
Size: 32 bits

Bit	Description
31:16	Reserved
15:3	**Base Address** — R/W. This field provides the base address of the I/O space (8 consecutive I/O locations).
2:1	Reserved
0	**Resource Type Indicator (RTE)** — RO. Hardwired to 1 to indicate a request for I/O space.

Note: This 8-byte I/O space is used in native mode for the Secondary Controller's Command Block.



8.1.14 SCNL_BAR—Secondary Control Block Base Address Register (SATA D31:F2)

Address Offset:	1Ch–1Fh	Attribute:	R/W, RO
Default Value:	00000001h	Size:	32 bits

Bit	Description
31:16	Reserved
15:2	**Base Address** — R/W. This field provides the base address of the I/O space (4 consecutive I/O locations).
1	Reserved
0	**Resource Type Indicator (RTE)** — RO. Hardwired to 1 to indicate a request for I/O space.

Note: This 4-byte I/O space is used in native mode for the Secondary Controller's Control Block.

8.1.15 BAR—Legacy Bus Master Base Address Register (SATA–D31:F2)

Address Offset:	20h–23h	Attribute:	R/W, RO
Default Value:	00000001h	Size:	32 bits

The Bus Master IDE interface function uses Base Address register 5 to request a 16-byte I/O space to provide a software interface to the Bus Master functions. Only 12 bytes are actually used (6 bytes for primary, 6 bytes for secondary). Only bits [15:4] are used to decode the address.

Bit	Description
31:16	Reserved
15:5	**Base Address** — R/W. This field provides the base address of the I/O space (16 consecutive I/O locations).
4	**Base**— R/W / RO. When SCC is 01h, this bit will be R/W resulting in requesting 16B of I/O space. When SCC is not 01h, this bit will be Read Only 0, resulting in requesting 32B of I/O space.
3:1	Reserved
0	**Resource Type Indicator (RTE)** — RO. Hardwired to 1 to indicate a request for I/O space.

8.1.16 ABAR/SIDPBA1—AHCI Base Address Register / Serial ATA Index Data Pair Base Address (SATA–D31:F2)

When the programming interface is not IDE (that is, SCC is not 01h), this register is named ABAR. When the programming interface is IDE, this register becomes SIDPBA.

Hardware does not clear those BA bits when switching from IDE component to non-IDE component or vice versa. BIOS is responsible for clearing those bits to 0 since the number of writable bits changes after component switching (as indicated by a change in SCC). In the case, this register will then have to be re-programmed to a proper value.

8.1.16.1 When SCC is not 01h

When the programming interface is not IDE, the register represents a memory BAR allocating space for the AHCI memory registers defined in Section 8.4.

Address Offset:	24–27h	Attribute:	R/W, RO
Default Value:	00000000h	Size:	32 bits

Bit	Description
31:11	**Base Address (BA)** — R/W. Base address of register memory space (aligned to 2 KB)
10:4	Reserved
3	**Prefetchable (PF)** — RO. Indicates that this range is not pre-fetchable
2:1	**Type (TP)** — RO. Indicates that this range can be mapped anywhere in 32-bit address space.
0	**Resource Type Indicator (RTE)** — RO. Hardwired to 0 to indicate a request for register memory space.

Note: The ABAR register must be set to a value of 0001_0000h or greater.

8.1.16.2 When SCC is 01h

When the programming interface is IDE, the register becomes an I/O BAR allocating 16 bytes of I/O space for the I/O-mapped registers defined in Section 8.2. Although 16 bytes of locations are allocated, only 8 bytes are used as SINDX and SDATA registers; with the remaining 8 bytes preserved for future enhancement.

Address Offset:	24h–27h	Attribute:	R/WO
Default Value:	00000001h	Size:	32 bits

Bit	Description
31:16	Reserved
15:4	**Base Address (BA)** — R/W. Base address of the I/O space.
3:1	Reserved
0	**Resource Type Indicator (RTE)** — RO. Indicates a request for I/O space.

8.1.17 SVID—Subsystem Vendor Identification Register (SATA–D31:F2)

Address Offset:	2Ch–2Dh	Attribute:	R/WO
Default Value:	0000h	Size:	16 bits
Lockable:	No	Power Well:	Core
Function Level Reset:	No		

Bit	Description
15:0	**Subsystem Vendor ID (SVID)** — R/WO. Value is written by BIOS. No hardware action taken on this value.

8.1.18 SID—Subsystem Identification Register (SATA–D31:F2)

Address Offset:	2Eh–2Fh	Attribute:	R/WO
Default Value:	0000h	Size:	16 bits
Lockable:	No	Power Well:	Core
Function Level Reset:	No		

Bit	Description
15:0	**Subsystem ID (SID)** — R/WO. Value is written by BIOS. No hardware action taken on this value.

8.1.19 CAP—Capabilities Pointer Register (SATA–D31:F2)

Address Offset: 34h
Default Value: 80h
Attribute: RO
Size: 8 bits

Bit	Description
7:0	**Capabilities Pointer (CAP_PTR)** — RO. Indicates that the first capability pointer offset is 80h. This value changes to 70h if the Sub Class Code (SCC) (Dev 31:F2:0Ah) is configure as IDE mode (value of 01).

8.1.20 INT_LN—Interrupt Line Register (SATA–D31:F2)

Address Offset: 3Ch
Default Value: 00h
Attribute: R/W
Size: 8 bits
Function Level Reset:No

Bit	Description
7:0	**Interrupt Line** — R/W. This field is used to communicate to software the interrupt line that the interrupt pin is connected to. Interrupt Line register is not reset by FLR.

8.1.21 INT_PN—Interrupt Pin Register (SATA–D31:F2)

Address Offset: 3Dh
Default Value: See Register Description
Attribute: RO
Size: 8 bits

Bit	Description
7:0	**Interrupt Pin** — RO. This reflects the value of D31IP.SIP (Chipset Config Registers:Offset 3100h:bits 11:8).

8.1.22 IDE_TIM—IDE Timing Register (SATA–D31:F2)

Address Offset: Primary: 40h–41h
Secondary: 42h–43h
Default Value: 0000h
Attribute: R/W
Size: 16 bits

Bits 14:12 and 9:0 of this register are R/W to maintain software compatibility. These bits have no effect on hardware.

Bit	Description
15	**IDE Decode Enable (IDE)** — R/W. Individually enable/disable the Primary or Secondary decode. 0 = Disable. 1 = Enables Intel® Xeon® Processor D-1500 Product Family to decode the associated Command Block (1F0–1F7h for primary, 170–177h for secondary, or their native mode BAR equivalents) and Control Block (3F6h for primary, 376h for secondary, or their native mode BAR equivalents). This bit effects the IDE decode ranges for both legacy and native-mode decoding.
14:12	**IDE_TIM Field 2** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.
11:10	Reserved
9:0	**IDE_TIM Field 1** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.

8.1.23 SIDETIM—Slave IDE Timing Register (SATA–D31:F2)

Address Offset: 44h
Default Value: 00h
Attribute: R/W
Size: 8 bits

Note: This register is R/W to maintain software compatibility. These bits have no effect on hardware.

Bit	Description
7:0	**SIDETIM Field 1** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.

8.1.24 SDMA_CNT—Synchronous DMA Control Register (SATA–D31:F2)

Address Offset: 48h
Default Value: 00h
Attribute: R/W
Size: 8 bits

Note: This register is R/W to maintain software compatibility. These bits have no effect on hardware.

Bit	Description
7:4	Reserved
3:0	**SDMA_CNT Field 1** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.

8.1.25 SDMA_TIM—Synchronous DMA Timing Register (SATA–D31:F2)

Address Offset: 4Ah–4Bh
Default Value: 0000h
Attribute: R/W
Size: 16 bits

Note: This register is R/W to maintain software compatibility. These bits have no effect on hardware.

Bit	Description
15:14	Reserved
13:12	**SDMA_TIM Field 4**— R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.
11:10	Reserved
9:8	**SDMA_TIM Field 3**— R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.
7:6	Reserved
5:4	**SDMA_TIM Field 2**— R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.
3:2	Reserved
1:0	**SDMA_TIM Field 1** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.

8.1.26 IDE_CONFIG—IDE I/O Configuration Register (SATA–D31:F2)

Address Offset: 54h–57h
Attribute: R/W
Default Value: 00000000h
Size: 32 bits

Note: This register is R/W to maintain software compatibility. These bits have no effect on hardware.

Bit	Description
31:24	Reserved
23:12	**IDE_CONFIG Field 2** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.
11:8	Reserved
7:0	**IDE_CONFIG Field 1** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.

8.1.27 PID—PCI Power Management Capability Identification Register (SATA–D31:F2)

Address Offset: 70h–71h
Attribute: RO
Default Value: See Register Description
Size: 16 bits

Bits	Description
15:8	**Next Capability (NEXT)** — R/W. A8h is the location of the Serial ATA capability structure. A8h is the recommended setting for non-IDE mode. If the controller is to operate in IDE mode, BIOS is requested to program this field to 00h. ***Note:*** Refer to the SGC.REGLOCK description in order to lock the register to become RO.
7:0	**Capability ID (CID)** — RO. Hardwired to 01h. Indicates that this pointer is a PCI power management.

8.1.28 PC—PCI Power Management Capabilities Register (SATA–D31:F2)

Address Offset: 72h–73h
Attribute: RO
Default Value: See Register Description
Size: 16 bits

Bits	Description
15:11	**PME Support (PME_SUP)** — RO. 00000 = If SCC = 01h, indicates no PME support in IDE mode. 01000 = If SCC is not 01h, in a non-IDE mode, indicates PME# can be generated from the $D3_{HOT}$ state in the SATA host controller.
10	**D2 Support (D2_SUP)** — RO. Hardwired to 0. The D2 state is not supported
9	**D1 Support (D1_SUP)** — RO. Hardwired to 0. The D1 state is not supported
8:6	**Auxiliary Current (AUX_CUR)** — RO. PME# from D3COLD state is not supported, therefore this field is 000b.
5	**Device Specific Initialization (DSI)** — RO. Hardwired to 0 to indicate that no device-specific initialization is required.
4	Reserved
3	**PME Clock (PME_CLK)** — RO. Hardwired to 0 to indicate that PCI clock is not required to generate PME#.
2:0	**Version (VER)** — RO. Hardwired to 011 to indicates support for Revision 1.2 of the PCI Power Management Specification.

8.1.29 PMCS—PCI Power Management Control and Status Register (SATA–D31:F2)

Address Offset: 74h–75h
Attribute: R/W, R/WC
Default Value: 0008h
Size: 16 bits
Function Level Reset: No (Bits 8 and 15)

Bits	Description
15	**PME Status (PMES)** — R/WC. Bit is set when a PME event is to be requested, and if this bit and PMEE is set, a PME# will be generated from the SATA controller ***Note:*** When SCC = 01h, hardware will automatically change the attribute of this bit to RO 0. Software is advised to clear PMEE and PMES together prior to changing SCC thru MAP.SMS. This bit is not reset by Function Level Reset.
14:9	Reserved
8	**PME Enable (PMEE)** — R/W. When set, the SATA controller asserts PME# when exiting $D3_{HOT}$ on a wake event. ***Note:*** When SCCSCC = 01h, hardware will automatically change the attribute of this bit to RO 0. Software is advised to clear PMEE and PMES together prior to changing SCC thru MAP.SMS. This bit is not reset by Function Level Reset.
7:4	Reserved
3	**No Soft Reset (NSFRST)** — RO. These bits are used to indicate whether devices transitioning from $D3_{HOT}$ state to D0 state will perform an internal reset. 0 = Device transitioning from $D3_{HOT}$ state to D0 state perform an internal reset. 1 = Device transitioning from $D3_{HOT}$ state to D0 state do not perform an internal reset. Configuration content is preserved. Upon transition from the $D3_{HOT}$ state to D0 state initialized state, no additional operating system intervention is required to preserve configuration context beyond writing to the PowerState bits. Regardless of this bit, the controller transition from $D3_{HOT}$ state to D0 state by a system or bus segment reset will return to the state D0 uninitialized with only PME context preserved if PME is supported and enabled.
2	Reserved
1:0	**Power State (PS)** — R/W. These bits are used both to determine the current power state of the SATA controller and to set a new power state. 00 = D0 state 11 = $D3_{HOT}$ state When in the $D3_{HOT}$ state, the controller's configuration space is available; however, the I/O and memory spaces are not. Additionally, interrupts are blocked.

8.1.30 MSICI—Message Signaled Interrupt Capability Identification Register (SATA–D31:F2)

Address Offset: 80h–81h
Attribute: RO
Default Value: 7005h
Size: 16 bits

Note: There is no support for MSI when the software is operating in legacy (IDE) mode when AHCI is not enabled. Prior to switching from AHCI to IDE mode, software **must** make sure that MSI is disabled.

Bits	Description
15:8	**Next Pointer (NEXT)** — R/W. Indicates the next item in the list is the PCI power management pointer. BIOS may program this field to A8h indicating that the next item is Serial ATA Capability Structure. ***Note:*** Refer to the SGC.REGLOCK description in order to lock the register to become RO. This bit is not reset by a Function Level Reset

Bits	Description
7:0	**Capability ID (CID)** — RO. Capabilities ID indicates MSI.

8.1.31 MSIMC—Message Signaled Interrupt Message Control Register (SATA–D31:F2)

Address Offset: 82h–83h
Default Value: 0000h
Attribute: R/W, RO
Size: 16 bits

Note: There is no support for MSI when the software is operating in legacy (IDE) mode when AHCI is not enabled. Prior to switching from AHCI to IDE mode, software **must** make sure that MSI is disabled.

<table>
<tr><th>Bits</th><th>Description</th></tr>
<tr><td>15:8</td><td>Reserved</td></tr>
<tr><td>7</td><td>64 Bit Address Capable (C64) — RO. Capable of generating a 32-bit message only.</td></tr>
<tr><td>6:4</td><td>Multiple Message Enable (MME) — RO.
= 000 (and MSIE is set), a single MSI message will be generated for all SATA ports, and bits [15:0] of the message vector will be driven from MD[15:0].
For 6 port components:
<table>
<tr><th rowspan="2">MME</th><th colspan="4">Value Driven on MSI Memory Write</th></tr>
<tr><th>Bits[15:3]</th><th>Bit[2]</th><th>Bit[1]</th><th>Bit[0]</th></tr>
<tr><td>000, 001, 010</td><td>MD[15:3]</td><td>MD[2]</td><td>MD[1]</td><td>MD[0]</td></tr>
<tr><td>011</td><td>MD[15:3]</td><td>Port 0: 0
Port 1: 0
Port 2: 0
Port 3: 0
Port 4: 1
Port 5: 1</td><td>Port 0: 0
Port 1: 0
Port 2: 1
Port 3: 1
Port 4: 0
Port 5: 0</td><td>Port 0: 0
Port 1: 1
Port 2: 0
Port 3: 1
Port 4: 0
Port 5: 1</td></tr>
</table>
For 4 port components:
<table>
<tr><th rowspan="2">MME</th><th colspan="4">Value Driven on MSI Memory Write</th></tr>
<tr><th>Bits[15:3]</th><th>Bit[2]</th><th>Bit[1]</th><th>Bit[0]</th></tr>
<tr><td>000, 001, 010</td><td>MD[15:3]</td><td>MD[2]</td><td>MD[1]</td><td>MD[0]</td></tr>
<tr><td>011</td><td>MD[15:3]</td><td>Port 0: 0
Port 1: 0
Port 4: 1
Port 5: 1</td><td>Port 0: 0
Port 1: 0
Port 2: 0
Port 3: 0</td><td>Port 0: 0
Port 1: 1
Port 2: 0
Port 3: 1</td></tr>
</table>
All other MME values are reserved. If this field is set to one of these reserved values, the results are undefined.
Note: The CCC interrupt is generated on unimplemented port (AHCI PI register bit equal to 0). If CCC interrupt is disabled, no MSI shall be generated for the port dedicated to the CCC interrupt. When CCC interrupt occurs, MD[2:0] is dependant on CCC_CTL.INT (in addition to MME).</td></tr>
<tr><td>3:1</td><td>Multiple Message Capable (MMC) — RO. MMC is not supported.</td></tr>
<tr><td>0</td><td>MSI Enable (MSIE) — R/W /RO. If set, MSI is enabled and traditional interrupt pins are not used to generate interrupts. This bit is R/W when SC.SCC is not 01h and is read-only 0 when SCC is 01h. The CMD.ID bit has no effect on MSI.

Note: Software must clear this bit to 0 to disable MSI first before changing the number of messages allocated in the MMC field. Software must also make sure this bit is cleared to ‘0’ when operating in legacy mode (when GHC.AE = 0).</td></tr>
</table>

8.1.32 MSIMA— Message Signaled Interrupt Message Address Register (SATA–D31:F2)

Address Offset: 84h–87h Attribute: R/W
Default Value: 00000000h Size: 32 bits

Note: There is no support for MSI when the software is operating in legacy (IDE) mode when AHCI is not enabled. Prior to switching from AHCI to IDE mode, software **must** make sure that MSI is disabled.

Bits	Description
31:2	**Address (ADDR)** — R/W. Lower 32 bits of the system specified message address, always DWord aligned.
1:0	Reserved

8.1.33 MSIMD—Message Signaled Interrupt Message Data Register (SATA–D31:F2)

Address Offset: 88h–89h Attribute: R/W
Default Value: 0000h Size: 16 bits

Note: There is no support for MSI when the software is operating in legacy (IDE) mode when AHCI is not enabled. Prior to switching from AHCI to IDE mode, software **must** make sure that MSI is disabled.

Bits	Description
15:0	**Data (DATA)** — R/W. This 16-bit field is programmed by system software if MSI is enabled. Its content is driven onto the lower word of the data bus of the MSI memory write transaction. When the MME field is set to '001' or '010', bit [0] and bits [1:0] respectively of the MSI memory write transaction will be driven based on the source of the interrupt rather than from MD[2:0]. See the description of the MME field.

8.1.34 MAP—Address Map Register (SATA–D31:F2)

Address Offset: 90h Attribute: R/W, R/WO
Default Value: 0000h Size: 16 bits
Function Level Reset:No (Bits 7:5 and 13:8 only)

Bits	Description
15:8	Reserved
7:6	**SATA Mode Select (SMS)** — R/W. Software programs these bits to control the mode in which the SATA Controller should operate: 00b = IDE mode 01b = AHCI mode 10b = RAID mode 11b = Reserved ***Notes:*** 1. The SATA Function Device ID will change based on the value of this register. 2. When switching from AHCI or RAID mode to IDE mode, a 2 port SATA controller (Device 31, Function 5) will be enabled. 3. SW shall not manipulate SMS during runtime operation; that is. the OS will not do this. The BIOS may choose to switch from one mode to another during POST. These bits are not reset by Function Level Reset.

Bits	Description
5	**SATA Port-to-Controller Configuration (SC)** — R/W. This bit changes the number of SATA ports available within each SATA Controller. 0 = Up to 4 SATA ports are available for Controller 1 (Device 31 Function 2) with ports [3:0] and up to 2 SATA ports are available for Controller 2 (Device 31 Function 5) with ports [5:4]. 1 = Up to 6 SATA ports are available for Controller 1 (Device 31 Function 2) with ports [5:0] and no SATA ports are available for Controller 2 (Device 31 Function 5). ***Note:*** This bit should be set to 1 in AHCI/RAID mode. This bit is not reset by Function Level Reset.
4:0	Reserved

8.1.35 PCS—Port Control and Status Register (SATA–D31:F2)

Address Offset: 92h–93h
Attribute: R/W, RO
Default Value: 0000h
Size: 16 bits
Function Level Reset: No

By default, the SATA ports are set to the disabled state (bits [5:0] = 0). When enabled by software, the ports can transition between the on, partial, and slumber states and can detect devices. When disabled, the port is in the "off" state and cannot detect any devices.

If an AHCI-aware or RAID enabled operating system is being booted, then system BIOS shall insure that all supported SATA ports are enabled prior to passing control to the OS. Once the AHCI aware OS is booted, it becomes the enabling/disabling policy owner for the individual SATA ports. This is accomplished by manipulating a port's PxSCTL and PxCMD fields. Because an AHCI or RAID aware OS will typically not have knowledge of the PxE bits and because the PxE bits act as master on/off switches for the ports, pre-boot software must insure that these bits are set to 1 prior to booting the OS, regardless as to whether or not a device is currently on the port.

Bits	Description
15	**OOB Retry Mode (ORM)** — R/W. 0 = The SATA controller will not retry after an OOB failure 1 = The SATA controller will continue to retry after an OOB failure until successful (infinite retry)
14	Reserved
13	**Port 5 Present (P5P)** — RO. The status of this bit may change at any time. This bit is cleared when the port is disabled using P5E. This bit is not cleared upon surprise removal of a device. 0 = No device detected. 1 = The presence of a device on Port 5 has been detected.
12	**Port 4 Present (P4P)** — RO. The status of this bit may change at any time. This bit is cleared when the port is disabled using P4E. This bit is not cleared upon surprise removal of a device. 0 = No device detected. 1 = The presence of a device on Port 4 has been detected.
11	**Port 3 Present (P3P)** — RO. The status of this bit may change at any time. This bit is cleared when the port is disabled using P3E. This bit is not cleared upon surprise removal of a device. 0 = No device detected. 1 = The presence of a device on Port 3 has been detected.
10	**Port 2 Present (P2P)** — RO. The status of this bit may change at any time. This bit is cleared when the port is disabled using P2E. This bit is not cleared upon surprise removal of a device. 0 = No device detected. 1 = The presence of a device on Port 2 has been detected.
9	**Port 1 Present (P1P)** — RO. The status of this bit may change at any time. This bit is cleared when the port is disabled using P1E. This bit is not cleared upon surprise removal of a device. 0 = No device detected. 1 = The presence of a device on Port 1 has been detected.

Bits	Description
8	**Port 0 Present (P0P)** — RO. The status of this bit may change at any time. This bit is cleared when the port is disabled using P0E. This bit is not cleared upon surprise removal of a device. 0 = No device detected. 1 = The presence of a device on Port 0 has been detected.
7:6	Reserved
5	**Port 5 Enabled (P5E)** — R/W / RO. 0 = Disabled. The port is in the 'off' state and cannot detect any devices. 1 = Enabled. The port can transition between the on, partial, and slumber states and can detect devices. ***Notes:*** 1. This bit takes precedence over P5CMD.SUD (offset ABAR+398h:bit 1) 2. If MAP.SC is 0, SCC is 01h, MAP.SPD[5] is 1h,or set to a PCIe* Port then this bit will be read only 0.
4	**Port 4 Enabled (P4E)** — R/W / RO. 0 = Disabled. The port is in the 'off' state and cannot detect any devices. 1 = Enabled. The port can transition between the on, partial, and slumber states and can detect devices. ***Note:*** 1. This bit takes precedence over P4CMD.SUD (offset ABAR+318h:bit 1) 2. If MAP.SC is 0, SCC is 01h, MAP.SPD[4] is 1h,or set to a PCIe Port then this bit will be read only 0.
3	**Port 3 Enabled (P3E)** — R/W / RO. 0 = Disabled. The port is in the 'off' state and cannot detect any devices. 1 = Enabled. The port can transition between the on, partial, and slumber states and can detect devices. ***Notes:*** 1. This bit takes precedence over P3CMD.SUD (offset ABAR+298h:bit 1). When MAP.SPD[3] is 1 this is reserved and is read-only 0.
2	**Port 2 Enabled (P2E)** — R/W / RO. 0 = Disabled. The port is in the 'off' state and cannot detect any devices. 1 = Enabled. The port can transition between the on, partial, and slumber states and can detect devices. ***Notes:*** 1. This bit takes precedence over P2CMD.SUD (offset ABAR+218h:bit 1). When MAP.SPD[2] is 1 this is reserved and is read-only 0.
1	**Port 1 Enabled (P1E)** — R/W / RO. 0 = Disabled. The port is in the 'off' state and cannot detect any devices. 1 = Enabled. The port can transition between the on, partial, and slumber states and can detect devices. ***Note:*** This bit takes precedence over P1CMD.SUD (offset ABAR+198h:bit 1). When MAP.SPD[1] is 1 this is reserved and is read-only 0.
0	**Port 0 Enabled (P0E)** — R/W / RO. 0 = Disabled. The port is in the 'off' state and cannot detect any devices. 1 = Enabled. The port can transition between the on, partial, and slumber states and can detect devices. ***Note:*** This bit takes precedence over P0CMD.SUD (offset ABAR+118h:bit 1). When MAP.SPD[0] is 1 this is reserved and is read-only 0.

8.1.36 SCLKCG—SATA Clock Gating Control Register

Address Offset: 94h–97h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits

Bit	Description
31:30	Reserved
29:24	**Port Clock Disable (PCD)** — R/W. 0 = All clocks to the associated port logic will operate normally. 1 = The backbone clock driven to the associated port logic is gated and will not toggle. Bit 29: Port 5 Bit 28: Port 4 Bit 27: Port 3 BIt 26: Port 2 Bit 25: Port 1 Bit 24: Port 0 If a port is not available, software shall set the corresponding bit to 1. Software can also set the corresponding bits to 1 on ports that are disabled. Software cannot set the PCD [port x]=1 if the corresponding PCS.PxE=1 in either Dev31Func2 or Dev31Func5 (dual controller IDE mode) or AHCI GHC.PI[x] = "1".
23:0	Reserved

8.1.37 SGC—SATA General Configuration Register

Address Offset: 9Ch–9Fh
Default Value: 00000000h
Attribute: R/W, R/WO
Size: 32 bits
Function Level Reset: No

Bit	Description
31	**Register Lock (REGLOCK)** — R/WO. 0 = Will not lock CAP.CAP_PTR, PID.NEXT, MSICI.NEXT, or SATACR0.NEXT 1 = Setting this bit will lock CAP.CAP_PTR, PID.NEXT, MSICI.NEXT, and SATACR0.NEXT. Once locked these register bits will become RO. BIOS is requested to program this field prior to IOS handoff. This bit is not reset by a Function Level Reset.
30:8	Reserved
7	**Alternate ID Enable (AIE)** — R/WO. BIOS must write to this bit field.
6	**Alternate ID Select (AIES)** — R/WO. BIOS must write to this bit field.
5	Reserved - BIOS may write to this field.
4:1	Reserved
0	**SATA 4-port All Master Configuration Indicator (SATA4PMIND)** — RO. 0 = Normal configuration. 1 = Two IDE Controllers are implemented, each supporting two ports for a Primary Master and a Secondary Master. ***Note:*** BIOS must also make sure that corresponding port clocks are gated (using SCLKCG configuration register).

8.1.38 SATACR0—SATA Capability Register 0 (SATA–D31:F2)

Address Offset: A8h–ABh
Attribute: RO, R/WO
Default Value: 0010B012h
Size: 32 bits
Function Level Reset: No (Bits 15:8 only)

Note: This register is read-only 0 when SCC is 01h.

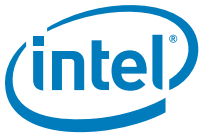
Bit	Description
31:24	Reserved
23:20	**Major Revision (MAJREV)** — RO. Major revision number of the SATA Capability Pointer implemented.
19:16	**Minor Revision (MINREV)** — RO. Minor revision number of the SATA Capability Pointer implemented.
15:8	**Next Capability Pointer (NEXT)** — R/WO. Points to the next capability structure. These bits are not reset by Function Level Reset.
7:0	**Capability ID (CAP)**— RW. The value 00h indicates the final item in the SATA Capability List. Refer to the SGC.REGLOCK description in order to lock the register to become RO.

8.1.39 SATACR1—SATA Capability Register 1 (SATA–D31:F2)

Address Offset: ACh–AFh
Attribute: RO
Default Value: 00000048h
Size: 32 bits

Note: When SCC is 01h, this register is read-only 0.

Bit	Description
31:16	Reserved
15:4	**BAR Offset (BAROFST)** — RO. Indicates the offset into the BAR where the Index/Data pair are located (in DWord granularity). The Index and Data I/O registers are located at offset 10h within the I/O space defined by LBAR. A value of 004h indicates offset 10h. 000h = 0h offset 001h = 4h offset 002h = 8h offset 003h = Bh offset 004h = 10h offset ... FFFh = 3FFFh offset (max 16KB)
3:0	**BAR Location (BARLOC)** — RO. Indicates the absolute PCI Configuration Register address of the BAR containing the Index/Data pair (in DWord granularity). The Index and Data I/O registers reside within the space defined by LBAR in the SATA controller. A value of 8h indicates offset 20h, which is LBAR. 0000 – 0011b = reserved 0100b = 10h => BAR0 0101b = 14h => BAR1 0110b = 18h => BAR2 0111b = 1Ch => BAR3 1000b = 20h => LBAR 1001b = 24h => BAR5 1010–1110b = Reserved 1111b = Index/Data pair in PCI Configuration space. This is not supported in Intel® Xeon® Processor D-1500 Product Family.



8.1.40 FLRCID—FLR Capability Identification Register (SATA–D31:F2)

Address Offset: B0–B1h Attribute: RO
Default Value: 0009h Size: 16 bits

Bit	Description
15:8	Next Capability Pointer — RO. 00h indicates the final item in the capability list.
7:0	**Capability ID** — RO. The value of this field depends on the FLRCSSEL (RCBA+3410h:bit 12) bit. **FLRCSSEL (RCBA+3410h:bit 12) Value** / **Capability ID Register Value** 0b / 13h 1b / 00h (Vendor Specific)

8.1.41 FLRCLV—FLR Capability Length and Version Register (SATA–D31:F2)

Address Offset: B2–B3h Attribute: RO, R/WO
Default Value: xx06h Size: 16 bits
Function Level Reset:No (Bit 9:8 Only when FLRCSSEL = 0)

When FLRCSSEL (RCBA+3410h:bit 12) = 1, this register is RO:

Bit	Description
15:10	Reserved
9	**FLR Capability** — R/WO. 1 = Support for Function Level reset. This bit is not reset by the Function Level Reset.
8	**TXP Capability** — R/WO. 1 = Support for Transactions Pending (TXP) bit. TXP must be supported if FLR is supported.
7:0	**Vendor-Specific Capability ID** — RO. This field indicates the number of bytes of this Vendor Specific capability as required by the PCI specification. It has the value of 06h for the FLR capability.

8.1.42 FLRC—FLR Control Register (SATA–D31:F2)

Address Offset: B4–B5h Attribute: RO, R/W
Default Value: 0000h Size: 16 bits

When FLRCSSEL (RCBA+3410h:bit 12) = 1, this register is RO.

Bit	Description
15:9	Reserved
8	**Transactions Pending (TXP)** — RO. 0 = Controller has received all non-posted requests. 1 = Controller has issued non-posted requests which has not been completed.
7:1	Reserved
0	**Initiate FLR** — R/W. Used to initiate FLR transition. A write of 1 indicates FLR transition. Since hardware must not respond to any cycles till FLR completion the value read by software from this bit is 0.

8.1.43 ATC—APM Trapping Control Register (SATA–D31:F2)

Address Offset: C0h
Default Value: 00h
Attribute: R/W
Size: 8 bits
Function Level Reset: No

Bit	Description
7:4	Reserved
3	**Secondary Slave Trap (SST)** — R/W. Enables trapping and SMI# assertion on legacy I/O accesses to 170h–177h and 376h. The active device on the secondary interface must be device 1 for the trap and/or SMI# to occur.
2	**Secondary Master Trap (SPT)** — R/W. Enables trapping and SMI# assertion on legacy I/O accesses to 170h-177h and 376h. The active device on the secondary interface must be device 0 for the trap and/or SMI# to occur.
1	**Primary Slave Trap (PST)** — R/W. Enables trapping and SMI# assertion on legacy I/O accesses to 1F0h–1F7h and 3F6h. The active device on the primary interface must be device 1 for the trap and/or SMI# to occur.
0	**Primary Master Trap (PMT)** — R/W. Enables trapping and SMI# assertion on legacy I/O accesses to 1F0h–1F7h and 3F6h. The active device on the primary interface must be device 0 for the trap and/or SMI# to occur.

8.1.44 ATS—APM Trapping Status Register (SATA–D31:F2)

Address Offset: C4h
Default Value: 00h
Attribute: R/WC
Size: 8 bits
Function Level Reset: No

Bit	Description
7:4	Reserved
3	**Secondary Slave Trap (SST)** — R/WC. Indicates that a trap occurred to the secondary slave device.
2	**Secondary Master Trap (SPT)** — R/WC. Indicates that a trap occurred to the secondary master device.
1	**Primary Slave Trap (PST)** — R/WC. Indicates that a trap occurred to the primary slave device.
0	**Primary Master Trap (PMT)** — R/WC. Indicates that a trap occurred to the primary master device.

8.1.45 SP—Scratch Pad Register (SATA–D31:F2)

Address Offset: D0h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits

Bit	Description
31:0	**Data (DT)** — R/W. This is a read/write register that is available for software to use. No hardware action is taken on this register.

8.1.46 BFCS—BIST FIS Control/Status Register (SATA–D31:F2)

Address Offset: E0h–E3h
Attribute: R/W, R/WC
Default Value: 00000000h
Size: 32 bits

Bits	Description
31:16	Reserved
15	**Port 5 BIST FIS Initiate (P5BFI)** — R/W. When a rising edge is detected on this bit field, Intel® Xeon® Processor D-1500 Product Family initiates a BIST FIS to the device on Port 5, using the parameters specified in this register and the data specified in BFTD1 and BFTD2. The BIST FIS will only be initiated if a device on Port 5 is present and ready (not partial/slumber state). After a BIST FIS is successfully completed, software must disable and re-enable the port using the PxE bits at offset 92h prior to attempting additional BIST FISs or to return Intel® Xeon® Processor D-1500 Product Family to a normal operational mode. If the BIST FIS fails to complete, as indicated by the BFF bit in the register, then software can clear then set the P5BFI bit to initiate another BIST FIS. This can be retried until the BIST FIS eventually completes successfully.
14	**Port 4 BIST FIS Initiate (P4BFI)** — R/W. When a rising edge is detected on this bit field, Intel® Xeon® Processor D-1500 Product Family initiates a BIST FIS to the device on Port 4, using the parameters specified in this register and the data specified in BFTD1 and BFTD2. The BIST FIS will only be initiated if a device on Port 4 is present and ready (not partial/slumber state). After a BIST FIS is successfully completed, software must disable and re-enable the port using the PxE bits at offset 92h prior to attempting additional BIST FISs or to return Intel® Xeon® Processor D-1500 Product Family to a normal operational mode. If the BIST FIS fails to complete, as indicated by the BFF bit in the register, then software can clear then set the P4BFI bit to initiate another BIST FIS. This can be retried until the BIST FIS eventually completes successfully.
13	**Port 3 BIST FIS Initiate (P3BFI)** — R/W. When a rising edge is detected on this bit field, Intel® Xeon® Processor D-1500 Product Family initiates a BIST FIS to the device on Port 3, using the parameters specified in this register and the data specified in BFTD1 and BFTD2. The BIST FIS will only be initiated if a device on Port 3 is present and ready (not partial/slumber state). After a BIST FIS is successfully completed, software must disable and re-enable the port using the PxE bits at offset 92h prior to attempting additional BIST FISs or to return Intel® Xeon® Processor D-1500 Product Family to a normal operational mode. If the BIST FIS fails to complete, as indicated by the BFF bit in the register, then software can clear then set the P3BFI bit to initiate another BIST FIS. This can be retried until the BIST FIS eventually completes successfully.
12	**Port 2 BIST FIS Initiate (P2BFI)** — R/W. When a rising edge is detected on this bit field, Intel® Xeon® Processor D-1500 Product Family initiates a BIST FIS to the device on Port 2, using the parameters specified in this register and the data specified in BFTD1 and BFTD2. The BIST FIS will only be initiated if a device on Port 2 is present and ready (not partial/slumber state). After a BIST FIS is successfully completed, software must disable and re-enable the port using the PxE bits at offset 92h prior to attempting additional BIST FISes or to return Intel® Xeon® Processor D-1500 Product Family to a normal operational mode. If the BIST FIS fails to complete, as indicated by the BFF bit in the register, then software can clear then set the P2BFI bit to initiate another BIST FIS. This can be retried until the BIST FIS eventually completes successfully.
11	**BIST FIS Successful (BFS)** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = This bit is set any time a BIST FIS transmitted by Intel® Xeon® Processor D-1500 Product Family receives an R_OK completion status from the device. ***Note:*** This bit must be cleared by software prior to initiating a BIST FIS.
10	**BIST FIS Failed (BFF)** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = This bit is set any time a BIST FIS transmitted by Intel® Xeon® Processor D-1500 Product Family receives an R_ERR completion status from the device. ***Note:*** This bit must be cleared by software prior to initiating a BIST FIS.
9	**Port 1 BIST FIS Initiate (P1BFI)** — R/W. When a rising edge is detected on this bit field, Intel® Xeon® Processor D-1500 Product Family initiates a BIST FIS to the device on Port 1, using the parameters specified in this register and the data specified in BFTD1 and BFTD2. The BIST FIS will only be initiated if a device on Port 1 is present and ready (not partial/slumber state). After a BIST FIS is successfully completed, software must disable and re-enable the port using the PxE bits at offset 92h prior to attempting additional BIST FISes or to return Intel® Xeon® Processor D-1500 Product Family to a normal operational mode. If the BIST FIS fails to complete, as indicated by the BFF bit in the register, then software can clear then set the P1BFI bit to initiate another BIST FIS. This can be retried until the BIST FIS eventually completes successfully.

Bits	Description
8	**Port 0 BIST FIS Initiate (P0BFI)** — R/W. When a rising edge is detected on this bit field, Intel® Xeon® Processor D-1500 Product Family initiates a BIST FIS to the device on Port 0, using the parameters specified in this register and the data specified in BFTD1 and BFTD2. The BIST FIS will only be initiated if a device on Port 0 is present and ready (not partial/slumber state). After a BIST FIS is successfully completed, software must disable and re-enable the port using the PxE bits at offset 92h prior to attempting additional BIST FISes or to return Intel® Xeon® Processor D-1500 Product Family to a normal operational mode. If the BIST FIS fails to complete, as indicated by the BFF bit in the register, then software can clear then set the P0BFI bit to initiate another BIST FIS. This can be retried until the BIST FIS eventually completes successfully.
7:2	**BIST FIS Parameters (BFP)** — R/W. These 6 bits form the contents of the upper 6 bits of the BIST FIS Pattern Definition in any BIST FIS transmitted by Intel® Xeon® Processor D-1500 Product Family. This field is not port specific — its contents will be used for any BIST FIS initiated on port 0, port 1, port 2, or port 3. The specific bit definitions are: Bit 7: T – Far End Transmit mode Bit 6: A – Align Bypass mode Bit 5: S – Bypass Scrambling Bit 4: L – Far End Retimed Loopback Bit 3: F – Far End Analog Loopback Bit 2: P – Primitive bit for use with Transmit mode
1:0	Reserved

8.1.47 BFTD1—BIST FIS Transmit Data1 Register (SATA–D31:F2)

Address Offset: E4h–E7h Attribute: R/W
Default Value: 00000000h Size: 32 bits

Bits	Description
31:0	**BIST FIS Transmit Data 1** — R/W. The data programmed into this register will form the contents of the second DWord of any BIST FIS initiated by Intel® Xeon® Processor D-1500 Product Family. This register is not port specific—its contents will be used for BIST FIS initiated on any port. Although the 2nd and 3rd DWs of the BIST FIS are only meaningful when the "T" bit of the BIST FIS is set to indicate "Far-End Transmit mode", this register's contents will be transmitted as the BIST FIS 2nd DW regardless of whether or not the "T" bit is indicated in the BFCS register (D31:F2:E0h).

8.1.48 BFTD2—BIST FIS Transmit Data2 Register (SATA–D31:F2)

Address Offset: E8h–EBh Attribute: R/W
Default Value: 00000000h Size: 32 bits

Bits	Description
31:0	**BIST FIS Transmit Data 2** — R/W. The data programmed into this register will form the contents of the third DWord of any BIST FIS initiated by Intel® Xeon® Processor D-1500 Product Family. This register is not port specific—its contents will be used for BIST FIS initiated on any port. Although the 2nd and 3rd DWs of the BIST FIS are only meaningful when the "T" bit of the BIST FIS is set to indicate "Far-End Transmit mode", this register's contents will be transmitted as the BIST FIS 3rd DW regardless of whether or not the "T" bit is indicated in the BFCS register (D31:F2:E0h).

8.2 Bus Master IDE I/O Registers (D31:F2)

The bus master IDE function uses 16 bytes of I/O space, allocated using the BAR register, located in D31:F2 Configuration space, offset 20h. All bus master IDE I/O space registers can be accessed as byte, word, or DWord quantities. Reading reserved bits returns an indeterminate, inconsistent value, and writes to reserved bits have no affect (but should not be attempted). These registers are only used for legacy operation. Software must not use these registers when running AHCI. All I/O registers are reset by Function Level Reset. The register address I/O map is shown in Table 8-2.

Table 8-2. Bus Master IDE I/O Register Address Map

BAR+ Offset	Mnemonic	Register	Default	Attribute
00h	BMICP	Command Register Primary	00h	R/W
01h	—	Reserved	—	RO
02h	BMISP	Bus Master IDE Status Register Primary	00h	R/W, R/WC, RO
03h	—	Reserved	—	RO
04h–07h	BMIDP	Bus Master IDE Descriptor Table Pointer Primary	xxxxxxxxh	R/W
08h	BMICS	Command Register Secondary	00h	R/W
09h	—	Reserved	—	RO
0Ah	BMISS	Bus Master IDE Status Register Secondary	00h	R/W, R/WC, RO
0Bh	—	Reserved	—	RO
0Ch–0Fh	BMIDS	Bus Master IDE Descriptor Table Pointer Secondary	xxxxxxxxh	R/W
10h	AIR	AHCI Index Register	00000000h	R/W, RO
14h	AIDR	AHCI Index Data Register	xxxxxxxxh	R/W

8.2.1 BMIC[P,S]—Bus Master IDE Command Register (D31:F2)

Address Offset: Primary: BAR + 00h
Secondary: BAR + 08h
Attribute: R/W
Default Value: 00h
Size: 8 bits

Bit	Description
7:4	Reserved. Returns 0.
3	**Read / Write Control (R/WC)** — R/W. This bit sets the direction of the bus master transfer. This bit must NOT be changed when the bus master function is active. 0 = Memory reads 1 = Memory writes
2:1	Reserved. Returns 0.

Bit	Description
0	**Start/Stop Bus Master (START)** — R/W. 0 = All state information is lost when this bit is cleared. Master mode operation cannot be stopped and then resumed. If this bit is reset while bus master operation is still active (that is, the Bus Master IDE Active bit (D31:F2:BAR + 02h, bit 0) of the Bus Master IDE Status register for that IDE channel is set) and the drive has not yet finished its data transfer (the Interrupt bit in the Bus Master IDE Status register for that IDE channel is not set), the bus master command is said to be aborted and data transferred from the drive may be discarded instead of being written to system memory. 1 = Enables bus master operation of the controller. Bus master operation does not actually start unless the Bus Master Enable bit (D31:F2:04h, bit 2) in PCI configuration space is also set. Bus master operation begins when this bit is detected changing from 0 to 1. The controller will transfer data between the IDE device and memory only when this bit is set. Master operation can be halted by writing a 0 to this bit. ***Note:*** This bit is intended to be cleared by software after the data transfer is completed, as indicated by either the Bus Master IDE Active bit being cleared or the Interrupt bit of the Bus Master IDE Status register for that IDE channel being set, or both. Hardware does not clear this bit automatically. If this bit is cleared to 0 prior to the DMA data transfer being initiated by the drive in a device to memory data transfer, then Intel® Xeon® Processor D-1500 Product Family will not send DMAT to terminate the data transfer. SW intervention (such as, sending SRST) is required to reset the interface in this condition.

8.2.2 BMIS[P,S]—Bus Master IDE Status Register (D31:F2)

Address Offset:	Primary: BAR + 02h Secondary: BAR + 0Ah	Attribute:	R/W, R/WC, RO
Default Value:	00h	Size:	8 bits

Bit	Description
7	**Simplex Only** — RO. 0 = Both bus master channels (primary and secondary) can be operated independently and can be used at the same time. 1 = Only one channel may be used at the same time.
6	**Drive 1 DMA Capable** — R/W. 0 = Not Capable. 1 = Capable. Set by device dependent code (BIOS or device driver) to indicate that drive 1 for this channel is capable of DMA transfers, and that the controller has been initialized for optimum performance. Intel® Xeon® Processor D-1500 Product Family does not use this bit. It is intended for systems that do not attach BMIDE to the PCI bus.
5	**Drive 0 DMA Capable** — R/W. 0 = Not Capable 1 = Capable. Set by device dependent code (BIOS or device driver) to indicate that drive 0 for this channel is capable of DMA transfers, and that the controller has been initialized for optimum performance. Intel® Xeon® Processor D-1500 Product Family does not use this bit. It is intended for systems that do not attach BMIDE to the PCI bus.
4:3	Reserved. Returns 0.
2	**Interrupt** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = Set when a device FIS is received with the 'I' bit set, provided that software has not disabled interrupts using the IEN bit of the Device Control Register.
1	**Error** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = This bit is set when the controller encounters a target abort or master abort when transferring data on PCI.
0	**Bus Master IDE Active (ACT)** — RO. 0 = This bit is cleared by Intel® Xeon® Processor D-1500 Product Family when the last transfer for a region is performed, where EOT for that region is set in the region descriptor. It is also cleared by Intel® Xeon® Processor D-1500 Product Family when the Start Bus Master bit (D31:F2:BAR+ 00h, bit 0) is cleared in the Command register. When this bit is read as a 0, all data transferred from the drive during the previous bus master command is visible in system memory, unless the bus master command was aborted. 1 = Set by Intel® Xeon® Processor D-1500 Product Family when the Start bit is written to the Command register.

8.2.3 BMID[P,S]—Bus Master IDE Descriptor Table Pointer Register (D31:F2)

Address Offset:	Primary: BAR + 04h–07h Secondary: BAR + 0Ch–0Fh	Attribute:	R/W
Default Value:	All bits undefined	Size:	32 bits

Bit	Description
31:2	**Address of Descriptor Table (ADDR)** — R/W. The bits in this field correspond to bits [31:2] of the memory location of the Physical Region Descriptor (PRD). The Descriptor Table must be DWord-aligned. The Descriptor Table must not cross a 64-K boundary in memory.
1:0	Reserved

8.2.4 AIR—AHCI Index Register (D31:F2)

Address Offset:	Primary: BAR + 10h	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits

This register is available only when SCC is not 01h.

Bit	Description
31:11	Reserved
10:2	**Index (INDEX)**— R/W. This Index register is used to select the DWord offset of the Memory Mapped AHCI register to be accessed. A DWord, Word or Byte access is specified by the active byte enables of the I/O access to the Data register.
1:0	Reserved

8.2.5 AIDR—AHCI Index Data Register (D31:F2)

Address Offset:	Primary: BAR + 14h	Attribute:	R/W
Default Value:	All bits undefined	Size:	32 bits

This register is available only when SCC is not 01h.

Bit	Description
31:0	**Data (DATA)**— R/W**:** This Data register is a "window" through which data is read or written to the AHCI memory mapped registers. A read or write to this Data register triggers a corresponding read or write to the memory mapped register pointed to by the Index register. The Index register must be setup prior to the read or write to this Data register. A physical register is not actually implemented as the data is actually stored in the memory mapped registers. Since this is not a physical register, the "default" value is the same as the default value of the register pointed to by Index.

8.3 Serial ATA Index/Data Pair Superset Registers

All of these I/O registers are in the core well. They are exposed only when SCC is 01h (that is, IDE programming interface).

These are Index/Data Pair registers that are used to access the SerialATA superset registers (SerialATA Status (PxSSTS), SerialATA Control (PxSCTL) and SerialATA Error (PxSERR)). The I/O space for these registers is allocated through SIDPBA. Locations with offset from 08h to 0Fh are reserved for future expansion. Software-write operations to the reserved locations will have no effect while software-read operations to the reserved locations will return 0.

Offset	Mnemonic	Register
00h–03h	SINDEX	Serial ATA Index
04h–07h	SDATA	Serial ATA Data
08h–0Ch	—	Reserved
0Ch–0Fh	—	Reserved

8.3.1 SINDX—Serial ATA Index Register (D31:F2)

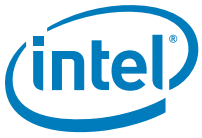
Address Offset: SIDPBA + 00h Attribute: R/W
Default Value: 00000000h Size: 32 bits

Bit	Description
31:16	Reserved
15.8	**Port Index (PIDX)**—R/W. This Index field is used to specify the port of the SATA controller at which the port-specific SSTS, SCTL, and SERR registers are located. 00h = Primary Master (Port 0) 01h = Primary Slave (Port 2) 02h = Secondary Master (Port 1) 03h = Secondary Slave (Port 3) All other values are Reserved.
7:0	**Register Index (RIDX)—**R/W. This index field is used to specify one out of three registers currently being indexed into. These three registers are the Serial ATA superset SStatus, SControl and SError memory registers and are port specific, hence for this SATA controller, there are four sets of these registers. Refer to Section 8.4.2.10, Section 8.4.2.11, and Section 8.4.2.12 for definitions of the SStatus, SControl and SError registers. 00h = SSTS 01h = SCTL 02h = SERR All other values are Reserved.

8.3.2 SDATA—Serial ATA Data Register (D31:F2)

Address Offset: SIDPBA + 04h Attribute: R/W
Default Value: 00000000h Size: 32 bits

Bit	Description
31:0	**Data (DATA)—**R/W. This Data register is a "window" through which data is read or written to from the register pointed to by the Serial ATA Index (SINDX) register above. A physical register is not actually implemented as the data is actually stored in the memory mapped registers. Since this is not a physical register, the "default" value is the same as the default value of the register pointed to by SINDX.RIDX field.



8.3.2.1 PxSSTS—Serial ATA Status Register (D31:F2)

Address Offset: Attribute: RO
Default Value: 00000000h Size: 32 bits

SDATA when SINDX.RIDX is 00h. This is a 32-bit register that conveys the current state of the interface and host. Intel® Xeon® Processor D-1500 Product Family updates it continuously and asynchronously. When Intel® Xeon® Processor D-1500 Product Family transmits a COMRESET to the device, this register is updated to its reset values.

Bit	Description
31:12	Reserved
11:8	**Interface Power Management (IPM)** — RO**.** Indicates the current interface state: **Value** — **Description** 0h — Device not present or communication not established 1h — Interface in active state 2h — Interface in PARTIAL power management state 6h — Interface in SLUMBER power management state All other values reserved.
7:4	**Current Interface Speed (SPD)** — RO. Indicates the negotiated interface communication speed. **Value** — **Description** 0h — Device not present or communication not established 1h — Generation 1 communication rate negotiated 2h — Generation 2 communication rate negotiated 3h — Generation 3 communication rate negotiated All other values reserved Intel® Xeon® Processor D-1500 Product Family Supports Generation 1 communication rates (1.5 Gb/s), Gen 2 rates (3.0 Gb/s) and Gen 3 rates (6.0Gb/s)
3:0	**Device Detection (DET)** — RO**.** Indicates the interface device detection and Phy state: **Value** — **Description** 0h — No device detected and Phy communication not established 1h — Device presence detected but Phy communication not established 3h — Device presence detected and Phy communication established 4h — Phy in offline mode as a result of the interface being disabled or running in a BIST loopback mode All other values reserved.

8.3.2.2 PxSCTL—Serial ATA Control Register (D31:F2)

Address Offset: Attribute: R/W, RO
Default Value: 00000000h Size: 32 bits

SDATA when SINDX.RIDX is 01h. This is a 32-bit read-write register by which software controls SATA capabilities. Writes to the SControl register result in an action being taken by Intel® Xeon® Processor D-1500 Product Family or the interface. Reads from the register return the last value written to it.

Bit	Description
31:20	Reserved
19:16	**Port Multiplier Port (PMP)** — R/W. This field is not used by AHCI.
15:12	**Select Power Management (SPM)** — R/W. This field is not used by AHCI.

Bit	Description
11:8	**Interface Power Management Transitions Allowed (IPM)** — R/W**.** Indicates which power states Intel® Xeon® Processor D-1500 Product Family is allowed to transition to: **Value** — **Description** 0h — No interface restrictions 1h — Transitions to the PARTIAL state disabled 2h — Transitions to the SLUMBER state disabled 3h — Transitions to both PARTIAL and SLUMBER states disabled All other values reserved
7:4	**Speed Allowed (SPD)** — R/W. Indicates the highest allowable speed of the interface. This speed is limited by the CAP.ISS (ABAR+00h:bit 23:20) field. **Value** — **Description** 0h — No speed negotiation restrictions 1h — Limit speed negotiation to Generation 1 communication rate 2h — Limit speed negotiation to Generation 2 communication rate 3h — Limit speed negotiation to Generation 3 communication rate All other values reserved. Intel® Xeon® Processor D-1500 Product Family Supports Generation 1 communication rates (1.5 Gb/s), Gen 2 rates (3.0 Gb/s) and Gen 3 rates (6.0Gb/s)
3:0	**Device Detection Initialization (DET)** — R/W. Controls Intel® Xeon® Processor D-1500 Product Family's device detection and interface initialization. **Value** — **Description** 0h — No device detection or initialization action requested 1h — Perform interface communication initialization sequence to establish communication. This is functionally equivalent to a hard reset and results in the interface being reset and communications re-initialized 4h — Disable the Serial ATA interface and put Phy in offline mode All other values reserved. When this field is written to a 1h, Intel® Xeon® Processor D-1500 Product Family initiates COMRESET and starts the initialization process. When the initialization is complete, this field shall remain 1h until set to another value by software. This field may only be changed to 1h or 4h when PxCMD.ST is 0. Changing this field while Intel® Xeon® Processor D-1500 Product Family is running results in undefined behavior.

8.3.2.3 PxSERR—Serial ATA Error Register (D31:F2)

Address Offset:		Attribute:	R/WC
Default Value:	00000000h	Size:	32 bits

SDATA when SINDx.RIDX is 02h.

Bits 26:16 of this register contains diagnostic error information for use by diagnostic software in validating correct operation or isolating failure modes. Bits 11:0 contain error information used by host software in determining the appropriate response to the error condition. If one or more of bits 11:8 of this register are set, the controller will stop the current transfer.

Bit	Description
31:27	Reserved
26	**Exchanged (X)**: When set to one, this bit indicates that a change in device presence has been detected since the last time this bit was cleared. This bit shall always be set to 1 anytime a COMINIT signal is received. This bit is reflected in the P0IS.PCS bit.
25	**Unrecognized FIS Type (F)**: Indicates that one or more FISs were received by the Transport layer with good CRC, but had a type field that was not recognized.

Bit	Description
24	**Transport state transition error (T)**: Indicates that an error has occurred in the transition from one state to another within the Transport layer since the last time this bit was cleared.
23	**Link Sequence Error (S):** Indicates that one or more Link state machine error conditions was encountered. The Link Layer state machine defines the conditions under which the link layer detects an erroneous transition.
22	**Handshake (H)**. Indicates that one or more R_ERR handshake response was received in response to frame transmission. Such errors may be the result of a CRC error detected by the recipient, a disparity or 8b/10b decoding error, or other error condition leading to a negative handshake on a transmitted frame.
21	**CRC Error (C)**. Indicates that one or more CRC errors occurred with the Link Layer.
20	**Disparity Error (D)**. This field is not used by AHCI.
19	**10b to 8b Decode Error (B)**. Indicates that one or more 10b to 8b decoding errors occurred.
18	**Comm Wake (W)**. Indicates that a Comm Wake signal was detected by the Phy.
17	**Phy Internal Error (I)**. Indicates that the Phy detected some internal error.
16	**PhyRdy Change (N)**: When set to 1, this bit indicates that the internal PhyRdy signal changed state since the last time this bit was cleared. In Intel® Xeon® Processor D-1500 Product Family, this bit will be set when PhyRdy changes from a 0 -> 1 or a 1 -> 0. The state of this bit is then reflected in the PxIS.PRCS interrupt status bit and an interrupt will be generated if enabled. Software clears this bit by writing a 1 to it.
15:12	Reserved
11	**Internal Error (E)**. The SATA controller failed due to a master or target abort when attempting to access system memory.
10	**Protocol Error (P)**. A violation of the Serial ATA protocol was detected. ***Note:*** Intel® Xeon® Processor D-1500 Product Family does not set this bit for all protocol violations that may occur on the SATA link.
9	**Persistent Communication or Data Integrity Error (C)**. A communication error that was not recovered occurred that is expected to be persistent. Persistent communications errors may arise from faulty interconnect with the device, from a device that has been removed or has failed, or a number of other causes.
8	**Transient Data Integrity Error (T)**: A data integrity error occurred that was not recovered by the interface.
7:2	Reserved
1	**Recovered Communications Error (M)**. Communications between the device and host was temporarily lost but was re-established. This can arise from a device temporarily being removed, from a temporary loss of Phy synchronization, or from other causes and may be derived from the PhyNRdy signal between the Phy and Link layers.
0	**Recovered Data Integrity Error (I)**. A data integrity error occurred that was recovered by the interface through a retry operation or other recovery action.

8.4 AHCI Registers (D31:F2)

Note: These registers are AHCI-specific and available when Intel® Xeon® Processor D-1500 Product Family is properly configured. The Serial ATA Status, Control, and Error registers are special exceptions and may be accessed on all Intel® Xeon® Processor D-1500 Product Family components if properly configured; see Section 8.3 for details.

The memory mapped registers within the SATA controller exist in non-cacheable memory space. Additionally, locked accesses are not supported. If software attempts to perform locked transactions to the registers, indeterminate results may occur. Register accesses shall have a maximum size of 64-bits; 64-bit access must not cross an 8-byte alignment boundary. All memory registers are reset by Function Level Reset unless specified otherwise.

The registers are broken into two sections – generic host control and port control. The port control registers are the same for all ports, and there are as many registers banks as there are ports.

Table 8-3. AHCI Register Address Map

ABAR + Offset	Mnemonic	Register
00–1Fh	GHC	Generic Host Control
20h–FFh	—	Reserved
100h–17Fh	P0PCR	Port 0 port control registers
180h–1FFh	P1PCR	Port 1 port control registers
200h–27Fh	P2PCR	Port 2 port control registers
280h–2FFh	P3PCR	Port 3 port control registers
300h–37Fh	P4PCR	Port 4 port control registers
380h–3FFh	P5PCR	Port 5 port control registers

8.4.1 AHCI Generic Host Control Registers (D31:F2)

Table 8-4. Generic Host Controller Register Address Map

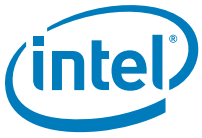
ABAR + Offset	Mnemonic	Register	Default	Attribute
00h–03h	CAP	Host Capabilities	FF22FFC2h	R/WO, RO
04h–07h	GHC	Global Intel® Xeon® Processor D-1500 Product Family Control	00000000h	R/W, RO
08h–0Bh	IS	Interrupt Status	00000000h	R/WC
0Ch–0Fh	PI	Ports Implemented	00000000h	R/WO, RO
10h–13h	VS	AHCI Version	00010300h	RO
1Ch–1Fh	EM_LOC	Enclosure Management Location	01600002h	RO
20h–23h	EM_CTRL	Enclosure Management Control	07010000h	R/W, R/WO, RO
24h–27h	CAP2	HBA Capabilities Extended	00000004h	RO

8.4.1.1 CAP—Host Capabilities Register (D31:F2)

Address Offset: ABAR + 00h–03h
Attribute: R/WO, RO
Default Value: FF22FFC2h
Size: 32 bits
Function Level Reset:No

All bits in this register that are R/WO are reset only by PLTRST#.

Bit	Description
31	**Supports 64-bit Addressing (S64A)** — RO. Indicates that the SATA controller can access 64-bit data structures. The 32-bit upper bits of the port DMA Descriptor, the PRD Base, and each PRD entry are read/write.
30	**Supports Command Queue Acceleration (SCQA)** — R/WO. When set to 1, indicates that the SATA controller supports SATA command queuing using the DMA Setup FIS. Intel® Xeon® Processor D-1500 Product Family handles DMA Setup FISes natively, and can handle auto-activate optimization through that FIS.
29	**Supports SNotification Register (SSNTF)** — R/WO. Intel® Xeon® Processor D-1500 Product Family SATA Controller does not support the SNotification register. BIOS must write a 0 to this field.
28	**Supports Mechanical Presence Switch (SMPS)** — R/WO. When set to 1, indicates whether the SATA controller supports mechanical presence switches on its ports for use in Hot-Plug operations. This value is loaded by platform BIOS prior to OS initialization. If this bit is set, BIOS must also map the SATAGP pins to the SATA controller through GPIO space.



Bit	Description
27	**Supports Staggered Spin-up (SSS)** — R/WO. Indicates whether the SATA controller supports staggered spin-up on its ports, for use in balancing power spikes. This value is loaded by platform BIOS prior to OS initialization. 0 = Staggered spin-up not supported. 1 = Staggered spin-up supported.
26	**Supports Aggressive Link Power Management (SALP)** — R/WO. 0 = Software shall treat the PxCMD.ALPE and PxCMD.ASP bits as reserved. 1 = The SATA controller supports auto-generating link requests to the partial or slumber states when there are no commands to process.
25	**Supports Activity LED (SAL)** — RO. Indicates that the SATA controller supports a single output pin (SATALED#) which indicates activity.
24	**Supports Command List Override (SCLO)** — R/WO. When set to 1, indicates that the Controller supports the PxCMD.CLO bit and its associated function. When cleared to 0, the Controller is not capable of clearing the BSY and DRQ bits in the Status register in order to issue a software reset if these bits are still set from a previous operation.
23:20	**Interface Speed Support (ISS)** — R/WO. Indicates the maximum speed the SATA controller can support on its ports. 1h = 1.5 Gb/s; 2h =3 Gb/s; 3h = 6 Gb/s
19	**Supports Non-Zero DMA Offsets (SNZO)** — RO. Reserved, as per the AHCI Revision 1.3 specification
18	**Supports AHCI Mode Only (SAM)** — RO. The SATA controller may optionally support AHCI access mechanism only. 0 = SATA controller supports both IDE and AHCI Modes 1 = SATA controller supports AHCI Mode Only
17:16	Reserved
15	**PIO Multiple DRQ Block (PMD)** — RO. Hardwired to 1. The SATA controller supports PIO Multiple DRQ Command Block
14	**Slumber State Capable (SSC)** — R/WO. When set to 1, the SATA controller supports the slumber state.
13	**Partial State Capable (PSC)** — R/WO. When set to 1, the SATA controller supports the partial state.
12:8	**Number of Command Slots (NCS)** — RO. Hardwired to 1Fh to indicate support for 32 slots.
7	**Command Completion Coalescing Supported (CCCS)** — R/WO. 0 = Command Completion Coalescing Not Supported 1 = Command Completion Coalescing Supported
6	**Enclosure Management Supported (EMS)** — R/WO. 0 = Enclosure Management Not Supported 1 = Enclosure Management Supported
5	**Supports External SATA (SXS)** — R/WO. 0 = External SATA is not supported on any ports 1 = External SATA is supported on one or more ports When set, software can examine each SATA port's Command Register (PxCMD) to determine which port is routed externally.
4:0	**Number of Ports (NPS)** — RO. Indicates number of supported ports. The number of ports indicated in this field may be more than the number of ports indicated in the PI (ABAR + 0Ch) register.

8.4.1.2 GHC—Global Intel® Xeon® Processor D-1500 Product Family Control Register (D31:F2)

Address Offset:	ABAR + 04h–07h	Attribute:	R/W, RO
Default Value:	00000000h	Size:	32 bits

Bit	Description
31	**AHCI Enable (AE)** — R/W. When set, this bit indicates that an AHCI driver is loaded and the controller will be talked to using AHCI mechanisms. This can be used by an Intel® Xeon® Processor D-1500 Product Family that supports both legacy mechanisms (such as SFF-8038i) and AHCI to know when the controller will not be talked to as legacy. 0 = Software will communicate with Intel® Xeon® Processor D-1500 Product Family using legacy mechanisms. 1 = Software will communicate with Intel® Xeon® Processor D-1500 Product Family using AHCI. Intel® Xeon® Processor D-1500 Product Family will not have to allow command processing using both AHCI and legacy mechanisms. Software shall set this bit to 1 before accessing other AHCI registers.
30:3	Reserved
2	**MSI Revert to Single Message (MRSM)** — RO: When set to 1 by hardware, this bit indicates that the host controller requested more than one MSI vector but has reverted to using the first vector only. When this bit is cleared to 0, the controller has not reverted to single MSI mode (that is, hardware is already in single MSI mode, software has allocated the number of messages requested, or hardware is sharing interrupt vectors if MC.MME < MC.MMC). "MC.MSIE = 1 (MSI is enabled) "MC.MMC > 0 (multiple messages requested) "MC.MME > 0 (more than one message allocated) "MC.MME!= MC.MMC (messages allocated not equal to number requested) When this bit is set to 1, single MSI mode operation is in use and software is responsible for clearing bits in the IS register to clear interrupts. This bit shall be cleared to 0 by hardware when any of the four conditions stated is false. This bit is also cleared to 0 when MC.MSIE = 1 and MC.MME = 0h. In this case, the hardware has been programmed to use single MSI mode, and is not "reverting" to that mode. For Intel® Xeon® Processor D-1500 Product Family, the controller shall always revert to single MSI mode when the number of vectors allocated by the host is less than the number requested. This bit is ignored when GHC.HR = 1.
1	**Interrupt Enable (IE)** — R/W. This global bit enables interrupts from Intel® Xeon® Processor D-1500 Product Family. 0 = All interrupt sources from all ports are disabled. 1 = Interrupts are allowed from the AHCI controller.
0	**Controller Reset (HR)** — R/W. Resets Intel® Xeon® Processor D-1500 Product Family AHCI controller. 0 = No effect 1 = When set by software, this bit causes an internal reset of Intel® Xeon® Processor D-1500 Product Family AHCI controller. All state machines that relate to data transfers and queuing return to an idle condition, and all ports are re-initialized using COMRESET. ***Note:*** For further details, consult Section 10.4.3 of the *Serial ATA Advanced Host Controller Interface Specification, Revision 1.3*.

8.4.1.3 IS—Interrupt Status Register (D31:F2)

Address Offset:	ABAR + 08h–0Bh	Attribute:	R/WC
Default Value:	00000000h	Size:	32 bits

This register indicates which of the ports within the controller have an interrupt pending and require service.

Bit	Description
31:6	Reserved. Returns 0.
5	**Interrupt Pending Status Port[5] (IPS[5])** — R/WC. 0 = No interrupt pending. 1 = Port 5 has an interrupt pending. Software can use this information to determine which ports require service after an interrupt.

Bit	Description
4	**Interrupt Pending Status Port[4] (IPS[4])** — R/WC. 0 = No interrupt pending. 1 = Port 4 has an interrupt pending. Software can use this information to determine which ports require service after an interrupt.
3	**Interrupt Pending Status Port[3] (IPS[3])** — R/WC. 0 = No interrupt pending. 1 = Port 3 has an interrupt pending. Software can use this information to determine which ports require service after an interrupt.
2	**Interrupt Pending Status Port[2] (IPS[2])** — R/WC. 0 = No interrupt pending. 1 = Port 2 has an interrupt pending. Software can use this information to determine which ports require service after an interrupt.
1	**Interrupt Pending Status Port[1] (IPS[1])** — R/WC. 0 = No interrupt pending. 1 = Port 1has an interrupt pending. Software can use this information to determine which ports require service after an interrupt.
0	**Interrupt Pending Status Port[0] (IPS[0])** — R/WC. 0 = No interrupt pending. 1 = Port 0 has an interrupt pending. Software can use this information to determine which ports require service after an interrupt.

8.4.1.4 PI—Ports Implemented Register (D31:F2)

Address Offset: ABAR + 0Ch–0Fh
Attribute: R/WO, RO
Default Value: 00000000h
Size: 32 bits
Function Level Reset: No

This register indicates which ports are exposed to Intel® Xeon® Processor D-1500 Product Family. It is loaded by platform BIOS. It indicates which ports that the device supports are available for software to use. For ports that are not available, software must not read or write to registers within that port. After BIOS issues initial write to this register, BIOS is requested to issue two reads to this register. If BIOS accesses any of the port specific AHCI address range before setting PI bit, BIOS is required to read the PI register before the initial write to the PI register.

Bit	Description
31:6	Reserved. Returns 0.
5	**Ports Implemented Port 5 (PI5)** — R/WO. 0 = The port is not implemented. 1 = The port is implemented. This bit is read-only 0 if this is a PCIe Port, MAP.SC = 0 or SCC = 01h.
4	**Ports Implemented Port 4 (PI4)** — R/WO. 0 = The port is not implemented. 1 = The port is implemented. This bit is read-only 0 if this is a PCIe Port, MAP.SC = 0 or SCC = 01h.
3	**Ports Implemented Port 3 (PI3)** — R/WO. 0 = The port is not implemented. 1 = The port is implemented.
2	**Ports Implemented Port 2 (PI2)**— R/WO. 0 = The port is not implemented. 1 = The port is implemented.
1	**Ports Implemented Port 1 (PI1)** — R/WO. 0 = The port is not implemented. 1 = The port is implemented.
0	**Ports Implemented Port 0 (PI0)** — R/WO. 0 = The port is not implemented. 1 = The port is implemented.

8.4.1.5 VS—AHCI Version Register (D31:F2)

Address Offset:	ABAR + 10h–13h	Attribute:	RO
Default Value:	00010300h	Size:	32 bits

This register indicates the major and minor version of the AHCI specification. It is BCD encoded. The upper two bytes represent the major version number, and the lower two bytes represent the minor version number. Example: Version 3.12 would be represented as 00030102h. The current version of the specification is 1.30 (00010300h).

Bit	Description
31:16	**Major Version Number (MJR)** — RO. Indicates the major version is 1
15:0	**Minor Version Number (MNR)** — RO. Indicates the minor version is 30.

8.4.1.6 EM_LOC—Enclosure Management Location Register (D31:F2)

Address Offset:	ABAR + 1Ch–1Fh	Attribute:	RO
Default Value:	01600002h	Size:	32 bits

This register identifies the location and size of the enclosure management message buffer. This register is reserved if enclosure management is not supported (that is, CAP.EMS = 0).

Bit	Description
31:16	**Offset (OFST)** — RO. The offset of the message buffer in DWords from the beginning of the ABAR.
15:0	**Buffer Size (SZ)** — RO. Specifies the size of the transmit message buffer area in DWords. Intel® Xeon® Processor D-1500 Product Family SATA controller only supports transmit buffer. A value of 0 is invalid.

8.4.1.7 EM_CTRL—Enclosure Management Control Register (D31:F2)

Address Offset:	ABAR + 20h–23h	Attribute:	R/W, R/WO, RO
Default Value:	07010000h	Size:	32 bits

This register is used to control and obtain status for the enclosure management interface. This register includes information on the attributes of the implementation, enclosure management messages supported, the status of the interface, whether any message are pending, and is used to initiate sending messages. This register is reserved if enclosure management is not supported (CAP_EMS = 0).

Bit	Description
31:27	Reserved
26	**Activity LED Hardware Driven (ATTR.ALHD)** — R/WO. 1 = The SATA controller drives the activity LED for the LED message type in hardware and does not utilize software for this LED. The host controller does not begin transmitting the hardware based activity signal until after software has written CTL.TM=1 after a reset condition.
25	**Transmit Only (ATTR.XMT)** — RO. 0 = The SATA controller supports transmitting and receiving messages. 1 = The SATA controller only supports transmitting messages and does not support receiving messages.
24	**Single Message Buffer (ATTR.SMB)** — RO. 0 = There are separate receive and transmit buffers such that unsolicited messages could be supported. 1 = The SATA controller has one message buffer that is shared for messages to transmit and messages received. Unsolicited receive messages are not supported and it is software's responsibility to manage access to this buffer.
23:20	Reserved

Bit	Description
19	**SGPIO Enclosure Management Messages (SUPP.SGPIO)** — RO. 1 = The SATA controller supports the SGPIO register interface message type.
18	**SES-2 Enclosure Management Messages (SUPP.SES2)** — RO. 1 = The SATA controller supports the SES-2 message type.
17	**SAF-TE Enclosure Management Messages (SUPP.SAFTE)** — RO. 1 = The SATA controller supports the SAF-TE message type.
16	**LED Message Types (SUPP.LED)** — RO. 1 = The SATA controller supports the LED message type.
15:10	Reserved
9	**Reset (RST):** — R/W. 0 = A write of 0 to this bit by software will have no effect. 1 = When set by software, The SATA controller resets all enclosure management message logic and takes all appropriate reset actions to ensure messages can be transmitted / received after the reset. After the SATA controller completes the reset operation, the SATA controller sets the value to 0.
8	**Transmit Message (CTL.TM)** — R/W. 0 = A write of 0 to this bit by software will have no effect. 1 = When set by software, The SATA controller transmits the message contained in the message buffer. When the message is completely sent, the SATA controller sets the value to 0. Software must not change the contents of the message buffer while CTL.TM is set to 1.
7:1	Reserved
0	**Message Received (STS.MR):** — RO. Message Received is not supported in Intel® Xeon® Processor D-1500 Product Family.

8.4.1.8 CAP2—HBA Capabilities Extended Register

Address Offset: ABAR + 24h–27h Attribute: RO
Default Value: 00000004h Size: 32 bits
Function Level Reset:No

Bit	Description
31:3	Reserved
2	**Automatic Partial to Slumber Transitions (APST)** 0= Not supported 1= Supported
1:0	Reserved

8.4.2 Port Registers (D31:F2)

Ports not available will result in the corresponding Port DMA register space being reserved. The controller shall ignore writes to the reserved space on write cycles and shall return 0 on read cycle accesses to the reserved location.

Table 8-5. Port [5:0] DMA Register Address Map (Sheet 1 of 3)

ABAR + Offset	Mnemonic	Register
100h–103h	P0CLB	Port 0 Command List Base Address
104h–107h	P0CLBU	Port 0 Command List Base Address Upper 32-Bits
108h–10Bh	P0FB	Port 0 FIS Base Address
10Ch–10Fh	P0FBU	Port 0 FIS Base Address Upper 32-Bits
110h–113h	P0IS	Port 0 Interrupt Status
114h–117h	P0IE	Port 0 Interrupt Enable
118h–11Bh	P0CMD	Port 0 Command
11Ch–11Fh	—	Reserved

Table 8-5. Port [5:0] DMA Register Address Map (Sheet 2 of 3)

ABAR + Offset	Mnemonic	Register
120h–123h	P0TFD	Port 0 Task File Data
124h–127h	P0SIG	Port 0 Signature
128h–12Bh	P0SSTS	Port 0 Serial ATA Status
12Ch–12Fh	P0SCTL	Port 0 Serial ATA Control
130h–133h	P0SERR	Port 0 Serial ATA Error
134h–137h	P0SACT	Port 0 Serial ATA Active
138h–13Bh	P0CI	Port 0 Command Issue
13Ch–17Fh	—	Reserved
180h–183h	P1CLB	Port 1 Command List Base Address
184h–187h	P1CLBU	Port 1 Command List Base Address Upper 32-Bits
188h–18Bh	P1FB	Port 1 FIS Base Address
18Ch–18Fh	P1FBU	Port 1 FIS Base Address Upper 32-Bits
190h–193h	P1IS	Port 1 Interrupt Status
194h–197h	P1IE	Port 1 Interrupt Enable
198h–19Bh	P1CMD	Port 1 Command
19Ch–19Fh	—	Reserved
1A0h–1A3h	P1TFD	Port 1 Task File Data
1A4h–1A7h	P1SIG	Port 1 Signature
1A8h–1ABh	P1SSTS	Port 1 Serial ATA Status
1ACh–1AFh	P1SCTL	Port 1 Serial ATA Control
1B0h–1B3h	P1SERR	Port 1 Serial ATA Error
1B4h–1B7h	P1SACT	Port 1 Serial ATA Active
1B8h–1BBh	P1CI	Port 1 Command Issue
1BCh–1FFh	—	Reserved
200h–203h	P2CLB	Port 2 Command List Base Address
204h–207h	P2CLBU	Port 2 Command List Base Address Upper 32-Bits
208h–20Bh	P2FB	Port 2 FIS Base Address
20Ch–20Fh	P2FBU	Port 2 FIS Base Address Upper 32-Bits
210h–213h	P2IS	Port 2 Interrupt Status
214h–217h	P2IE	Port 2 Interrupt Enable
218h–21Bh	P2CMD	Port 2 Command
21Ch–21Fh	—	Reserved
220h–223h	P2TFD	Port 2 Task File Data
224h–227h	P2SIG	Port 2 Signature
228h–22Bh	P2SSTS	Port 2 Serial ATA Status
22Ch–22Fh	P2SCTL	Port 2 Serial ATA Control
230h–233h	P2SERR	Port 2 Serial ATA Error
234h–237h	P2SACT	Port 2 Serial ATA Active
238h–23Bh	P2CI	Port 2 Command Issue
23Ch–27Fh	—	Reserved
280h–283h	P3CLB	Port 3 Command List Base Address
284h–287h	P3CLBU	Port 3 Command List Base Address Upper 32-Bits
288h–28Bh	P3FB	Port 3 FIS Base Address
28Ch–28Fh	P3FBU	Port 3 FIS Base Address Upper 32-Bits

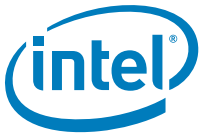


Table 8-5. Port [5:0] DMA Register Address Map (Sheet 3 of 3)

ABAR + Offset	Mnemonic	Register
290h–293h	P3IS	Port 3 Interrupt Status
294h–297h	P3IE	Port 3 Interrupt Enable
298h–29Bh	P3CMD	Port 3 Command
29Ch–29Fh	—	Reserved
2A0h–2A3h	P3TFD	Port 3 Task File Data
2A4h–2A7h	P3SIG	Port 3 Signature
2A8h–2ABh	P3SSTS	Port 3 Serial ATA Status
2ACh–2AFh	P3SCTL	Port 3 Serial ATA Control
2B0h–2B3h	P3SERR	Port 3 Serial ATA Error
2B4h–2B7h	P3SACT	Port 3 Serial ATA Active
2B8h–2BBh	P3CI	Port 3 Command Issue
2BCh–2FFh	—	Reserved
300h–303h	P4CLB	Port 4 Command List Base Address
304h–307h	P4CLBU	Port 4 Command List Base Address Upper 32-Bits
308h–30Bh	P4FB	Port 4 FIS Base Address
30Ch–30Fh	P4FBU	Port 4 FIS Base Address Upper 32-Bits
310h–313h	P4IS	Port 4 Interrupt Status
314h–317h	P4IE	Port 4 Interrupt Enable
318h–31Bh	P4CMD	Port 4 Command
31Ch–31Fh	—	Reserved
320h–323h	P4TFD	Port 4 Task File Data
324h–327h	P4SIG	Port 4 Signature
328h–32Bh	P4SSTS	Port 4 Serial ATA Status
32Ch–32Fh	P4SCTL	Port 4 Serial ATA Control
330h–333h	P4SERR	Port 4 Serial ATA Error
334h–337h	P4SACT	Port 4 Serial ATA Active
338h–33Bh	P4CI	Port 4 Command Issue
33Ch–37Fh	—	Reserved
380h–383h	P5CLB	Port 5 Command List Base Address
384h–387h	P5CLBU	Port 5 Command List Base Address Upper 32-Bits
388h–38Bh	P5FB	Port 5 FIS Base Address
38Ch–38Fh	P5FBU	Port 5 FIS Base Address Upper 32-Bits
390h–393h	P5IS	Port 5 Interrupt Status
394h–397h	P5IE	Port 5 Interrupt Enable
398h–39Bh	P5CMD	Port 5 Command
39Ch–39Fh	—	Reserved
3A0h–3A3h	P5TFD	Port 5 Task File Data
3A4h–3A7h	P5SIG	Port 5 Signature
3A8h–3ABh	P5SSTS	Port 5 Serial ATA Status
3ACh–3AFh	P5SCTL	Port 5 Serial ATA Control
3B0h–3B3h	P5SERR	Port 5 Serial ATA Error
3B4h–3B7h	P5SACT	Port 5 Serial ATA Active
3B8h–3BBh	P5CI	Port 5 Command Issue
3BCh–FFFh	—	Reserved

8.4.2.1 PxCLB—Port [5:0] Command List Base Address Register (D31:F2)

Address Offset: Port 0: ABAR + 100h
Port 1: ABAR + 180h
Port 2: ABAR + 200h (if port available; see Section 1.3)
Port 3: ABAR + 280h (if port available; see Section 1.3)
Port 4: ABAR + 300h
Port 5: ABAR + 380h
Attribute: R/W
Default Value: Undefined
Size: 32 bits

Bit	Description
31:10	**Command List Base Address (CLB)** — R/W. Indicates the 32-bit base for the command list for this port. This base is used when fetching commands to execute. The structure pointed to by this address range is 1 KB in length. This address must be 1 KB aligned as indicated by bits 31:10 being read/write. These bits are not reset on a controller reset.
9:0	Reserved

8.4.2.2 PxCLBU—Port [5:0] Command List Base Address Upper 32-Bits Register (D31:F2)

Address Offset: Port 0: ABAR + 104h
Port 1: ABAR + 184h
Port 2: ABAR + 204h (if port available; see Section 1.3)
Port 3: ABAR + 284h (if port available; see Section 1.3)
Port 4: ABAR + 304h
Port 5: ABAR + 384h
Attribute: R/W
Default Value: Undefined
Size: 32 bits

Bit	Description
31:0	**Command List Base Address Upper (CLBU)** — R/W. Indicates the upper 32-bits for the command list base address for this port. This base is used when fetching commands to execute. These bits are not reset on a controller reset.

8.4.2.3 PxFB—Port [5:0] FIS Base Address Register (D31:F2)

Address Offset: Port 0: ABAR + 108h
Port 1: ABAR + 188h
Port 2: ABAR + 208h (if port available; see Section 1.3)
Port 3: ABAR + 288h (if port available; see Section 1.3)
Port 4: ABAR + 308h
Port 5: ABAR + 388h
Attribute: R/W
Default Value: Undefined
Size: 32 bits

Bit	Description
31:8	**FIS Base Address (FB)** — R/W. Indicates the 32-bit base for received FISes. The structure pointed to by this address range is 256 bytes in length. This address must be 256-byte aligned, as indicated by bits 31:3 being read/write. These bits are not reset on a controller reset.
7:0	Reserved

8.4.2.4 PxFBU—Port [5:0] FIS Base Address Upper 32-Bits Register (D31:F2)

Address Offset: Port 0: ABAR + 10Ch — Attribute: R/W
Port 1: ABAR + 18Ch
Port 2: ABAR + 20Ch (if port available; see Section 1.3)
Port 3: ABAR + 28Ch (if port available; see Section 1.3)
Port 4: ABAR + 30Ch
Port 5: ABAR + 38Ch
Default Value: Undefined — Size: 32 bits

Bit	Description
31:0	**FIS Base Address Upper (FBU)** — R/W. Indicates the upper 32-bits for the received FIS base for this port. These bits are not reset on a controller reset.

8.4.2.5 PxIS—Port [5:0] Interrupt Status Register (D31:F2)

Address Offset: Port 0: ABAR + 110h — Attribute: R/WC, RO
Port 1: ABAR + 190h
Port 2: ABAR + 210h (if port available; see Section 1.3)
Port 3: ABAR + 290h (if port available; see Section 1.3)
Port 4: ABAR + 310h
Port 5: ABAR + 390h
Default Value: 00000000h — Size: 32 bits

Bit	Description
31	**Cold Port Detect Status (CPDS)** — RO. Cold presence detect is not supported.
30	**Task File Error Status (TFES)** — R/WC. This bit is set whenever the status register is updated by the device and the error bit (PxTFD.bit 0) is set.
29	**Host Bus Fatal Error Status (HBFS)** — R/WC. Indicates that Intel® Xeon® Processor D-1500 Product Family encountered an error that it cannot recover from due to a bad software pointer. In PCI, such an indication would be a target or master abort.
28	**Host Bus Data Error Status (HBDS)** — R/WC. Indicates that Intel® Xeon® Processor D-1500 Product Family encountered a data error (uncorrectable ECC / parity) when reading from or writing to system memory.
27	**Interface Fatal Error Status (IFS)** — R/WC. Indicates that Intel® Xeon® Processor D-1500 Product Family encountered an error on the SATA interface which caused the transfer to stop.
26	**Interface Non-fatal Error Status (INFS)** — R/WC. Indicates that Intel® Xeon® Processor D-1500 Product Family encountered an error on the SATA interface but was able to continue operation.
25	Reserved
24	**Overflow Status (OFS)** — R/WC. Indicates that Intel® Xeon® Processor D-1500 Product Family received more bytes from a device than was specified in the PRD table for the command.
23	**Incorrect Port Multiplier Status (IPMS)** — R/WC. Intel® Xeon® Processor D-1500 Product Family SATA controller does not support Port Multipliers.
22	**PhyRdy Change Status (PRCS)** — RO. When set to one, this bit indicates the internal PhyRdy signal changed state. This bit reflects the state of PxSERR.DIAG.N. Unlike most of the other bits in the register, this bit is RO and is only cleared when PxSERR.DIAG.N is cleared. The internal PhyRdy signal also transitions when the port interface enters partial or slumber power management states. Partial and slumber must be disabled when Surprise Removal Notification is desired, otherwise the power management state transitions will appear as false insertion and removal events.
21:8	Reserved
7	**Device Interlock Status (DIS)** — R/WC. When set, this bit indicates that a platform mechanical presence switch has been opened or closed, which may lead to a change in the connection state of the device. This bit is only valid in systems that support an mechanical presence switch (CAP.SIS [ABAR+00:bit 28] set). For systems that do not support an mechanical presence switch, this bit will always be 0.

Bit	Description
6	**Port Connect Change Status (PCS)** — RO**.** This bit reflects the state of PxSERR.DIAG.X. (ABAR+130h/1D0h/230h/2D0h, bit 26) Unlike other bits in this register, this bit is only cleared when PxSERR.DIAG.X is cleared. 0 = No change in Current Connect Status. 1 = Change in Current Connect Status.
5	**Descriptor Processed (DPS)** — R/WC. A PRD with the I bit set has transferred all its data.
4	**Unknown FIS Interrupt (UFS)** — RO. When set to 1, this bit indicates that an unknown FIS was received and has been copied into system memory. This bit is cleared to 0 by software clearing the PxSERR.DIAG.F bit to 0. This bit does not directly reflect the PxSERR.DIAG.F bit. PxSERR.DIAG.F is set immediately when an unknown FIS is detected, whereas this bit is set when the FIS is posted to memory. Software should wait to act on an unknown FIS until this bit is set to 1 or the two bits may become out of sync.
3	**Set Device Bits Interrupt (SdBS)** — R/WC. A Set Device Bits FIS has been received with the I bit set and has been copied into system memory.
2	**DMA Setup FIS Interrupt (DSS)** — R/WC. A DMA Setup FIS has been received with the I bit set and has been copied into system memory.
1	**PIO Setup FIS Interrupt (PSS)** — R/WC. A PIO Setup FIS has been received with the I bit set, it has been copied into system memory, and the data related to that FIS has been transferred.
0	**Device to Host Register FIS Interrupt (DHRS)** — R/WC. A D2H Register FIS has been received with the I bit set, and has been copied into system memory.

8.4.2.6 PxIE—Port [5:0] Interrupt Enable Register (D31:F2)

Address Offset: Port 0: ABAR + 114h — Attribute: R/W, RO
Port 1: ABAR + 194h
Port 2: ABAR + 214h (if port available; see Section 1.3)
Port 3: ABAR + 294h (if port available; see Section 1.3)
Port 4: ABAR + 314h
Port 5: ABAR + 394h
Default Value: 00000000h — Size: 32 bits

This register enables and disables the reporting of the corresponding interrupt to system software. When a bit is set (1) and the corresponding interrupt condition is active, then an interrupt is generated. Interrupt sources that are disabled (0) are still reflected in the status registers.

Bit	Description
31	**Cold Presence Detect Enable (CPDE)** — RO. Cold Presence Detect is not supported.
30	**Task File Error Enable (TFEE)** — R/W. When set, and GHC.IE and PxTFD.STS.ERR (due to a reception of the error register from a received FIS) are set, Intel® Xeon® Processor D-1500 Product Family will generate an interrupt.
29	**Host Bus Fatal Error Enable (HBFE)** — R/W. When set, and GHC.IE and PxS.HBFS are set, Intel® Xeon® Processor D-1500 Product Family will generate an interrupt.
28	**Host Bus Data Error Enable (HBDE)** — R/W. When set, and GHC.IE and PxS.HBDS are set, Intel® Xeon® Processor D-1500 Product Family will generate an interrupt.
27	**Host Bus Data Error Enable (HBDE)** — R/W. When set, GHC.IE is set, and PxIS.HBDS is set, Intel® Xeon® Processor D-1500 Product Family will generate an interrupt.
26	**Interface Non-fatal Error Enable (INFE)** — R/W. When set, GHC.IE is set, and PxIS.INFS is set, Intel® Xeon® Processor D-1500 Product Family will generate an interrupt.
25	Reserved
24	**Overflow Error Enable (OFE)** — R/W**.** When set, and GHC.IE and PxS.OFS are set, Intel® Xeon® Processor D-1500 Product Family will generate an interrupt.
23	**Incorrect Port Multiplier Enable (IPME)** — R/W. Intel® Xeon® Processor D-1500 Product Family SATA controller does not support Port Multipliers. BIOS and storage software should keep this bit cleared to 0.
22	**PhyRdy Change Interrupt Enable (PRCE)** — R/W. When set, and GHC.IE is set, and PxIS.PRCS is set, Intel® Xeon® Processor D-1500 Product Family shall generate an interrupt.
21:8	Reserved

Bit	Description
7	**Device Interlock Enable (DIE)** — R/W. When set, and PxIS.DIS is set, Intel® Xeon® Processor D-1500 Product Family will generate an interrupt. For systems that do not support an mechanical presence switch, this bit shall be a read-only 0.
6	**Port Change Interrupt Enable (PCE)** — R/W. When set, and GHC.IE and PxS.PCS are set, Intel® Xeon® Processor D-1500 Product Family will generate an interrupt.
5	**Descriptor Processed Interrupt Enable (DPE)** — R/W. When set, and GHC.IE and PxS.DPS are set, Intel® Xeon® Processor D-1500 Product Family will generate an interrupt.
4	**Unknown FIS Interrupt Enable (UFIE)** — R/W. When set, and GHC.IE is set and an unknown FIS is received, Intel® Xeon® Processor D-1500 Product Family will generate this interrupt.
3	**Set Device Bits FIS Interrupt Enable (SdBE)** — R/W. When set, and GHC.IE and PxS.SdBS are set, Intel® Xeon® Processor D-1500 Product Family will generate an interrupt.
2	**DMA Setup FIS Interrupt Enable (DSE)** — R/W. When set, and GHC.IE and PxS.DSS are set, Intel® Xeon® Processor D-1500 Product Family will generate an interrupt.
1	**PIO Setup FIS Interrupt Enable (PSE)** — R/W. When set, and GHC.IE and PxS.PSS are set, Intel® Xeon® Processor D-1500 Product Family will generate an interrupt.
0	**Device to Host Register FIS Interrupt Enable (DHRE)** — R/W. When set, and GHC.IE and PxS.DHRS are set, Intel® Xeon® Processor D-1500 Product Family will generate an interrupt.

8.4.2.7 PxCMD—Port [5:0] Command Register (D31:F2)

Address Offset: Port 0: ABAR + 118h — Attribute: R/W, RO, R/WO
Port 1: ABAR + 198h
Port 2: ABAR + 218h (if port available; see Section 1.3)
Port 3: ABAR + 298h (if port available; see Section 1.3)
Port 4: ABAR + 318h
Port 5: ABAR + 398h
Default Value: 0000w00wh — Size: 32 bits
where w = 00?0b (for?, see bit description)
Function Level Reset: No (Bit 21, 19 and 18 only)

Bit	Description
31:28	**Interface Communication Control (ICC)** — R/W.This is a four bit field that can be used to control reset and power states of the interface. Writes to this field will cause actions on the interface, either as primitives or an OOB sequence, and the resulting status of the interface will be reported in the PxSSTS register (Address offset Port 0:ABAR+124h, Port 1: ABAR+1A4h, Port 2: ABAR+224h, Port 3: ABAR+2A4h, Port 4: ABAR+224h, Port 5: ABAR+2A4h). **Value** — **Definition** Fh–7h — Reserved 6h — Slumber: This will cause Intel® Xeon® Processor D-1500 Product Family to request a transition of the interface to the slumber state. The SATA device may reject the request and the interface will remain in its current state 5h–3h — Reserved 2h — Partial: This will cause Intel® Xeon® Processor D-1500 Product Family to request a transition of the interface to the partial state. The SATA device may reject the request and the interface will remain in its current state. 1h — Active: This will cause Intel® Xeon® Processor D-1500 Product Family to request a transition of the interface into the active 0h — No-Op / Idle: When software reads this value, it indicates Intel® Xeon® Processor D-1500 Product Family is not in the process of changing the interface state or sending a device reset, and a new link command may be issued. When system software writes a non-reserved value other than No-Op (0h), Intel® Xeon® Processor D-1500 Product Family will perform the action and update this field back to Idle (0h). If software writes to this field to change the state to a state the link is already in (such as, interface is in the active state and a request is made to go to the active state), Intel® Xeon® Processor D-1500 Product Family will take no action and return this field to Idle. ***Note:*** When the ALPE bit (bit 26) is set, this register should not be set to 02h or 06h.

Bit	Description
27	**Aggressive Slumber / Partial (ASP)** — R/W. When set to 1, and the ALPE bit (bit 26) is set, Intel® Xeon® Processor D-1500 Product Family shall aggressively enter the slumber state when it clears the PxCI register and the PxSACT register is cleared. When cleared, and the ALPE bit is set, Intel® Xeon® Processor D-1500 Product Family will aggressively enter the partial state when it clears the PxCI register and the PxSACT register is cleared. If CAP.SALP is cleared to 0, software shall treat this bit as reserved.
26	**Aggressive Link Power Management Enable (ALPE)** — R/W. When set to 1, Intel® Xeon® Processor D-1500 Product Family will aggressively enter a lower link power state (partial or slumber) based upon the setting of the ASP bit (bit 27).
25	**Drive LED on ATAPI Enable (DLAE)** — R/W**.** When set to 1, Intel® Xeon® Processor D-1500 Product Family will drive the LED pin active for ATAPI commands (PxCLB[CHz.A] set) in addition to ATA commands. When cleared, Intel® Xeon® Processor D-1500 Product Family will only drive the LED pin active for ATA commands. See Section 3.15.9 for details on the activity LED.
24	**Device is ATAPI (ATAPI)** — R/W. When set to 1, the connected device is an ATAPI device. This bit is used by Intel® Xeon® Processor D-1500 Product Family to control whether or not to generate the server LED when commands are active. See Section 3.15.9 for details on the activity LED.
23	**Automatic Partial Slumber Transitions Enabled (APSTE)**— R/W. 0 = This port will not perform Automatic Partial to Slumber Transitions. 1 = The HBA may perform Automatic Partial to Slumber Transitions. ***Note:*** Software should only set this bit to '1' if CAP2.APST is set to '1'.
22	Reserved
21	**External SATA Port (ESP)** — R/WO. 0 = This port supports internal SATA devices only. 1 = This port will be used with an external SATA device and Hot-Plug is supported. When set, CAP.SXS must also be set. This bit is not reset by Function Level Reset.
20	Reserved
19	**Mechanical Switch Attached to Port (MPSP)** — R/WO. If set to 1, Intel® Xeon® Processor D-1500 Product Family supports a mechanical presence switch attached to this port. Intel® Xeon® Processor D-1500 Product Family takes no action on the state of this bit – it is for system software only. For example, if this bit is cleared, and an mechanical presence switch toggles, Intel® Xeon® Processor D-1500 Product Family still treats it as a proper mechanical presence switch event. ***Note:*** This bit is not reset on a Controller reset or by a Function Level Reset.
18	**Hot-Plug Capable Port (HPCP)** — R/WO. 0 = Port is not capable of Hot-Plug. 1 = Port is Hot-Plug capable. This indicates whether the platform exposes this port to a device which can be Hot-Plugged. SATA by definition is hot-pluggable, but not all platforms are constructed to allow the device to be removed (it may be screwed into the chassis, for example). This bit can be used by system software to indicate a feature such as "eject device" to the end-user. Intel® Xeon® Processor D-1500 Product Family takes no action on the state of this bit — it is for system software only. For example, if this bit is cleared, and a Hot-Plug event occurs, Intel® Xeon® Processor D-1500 Product Family still treats it as a proper Hot-Plug event. ***Note:*** This bit is not reset on a Controller reset or by a Function Level Reset.
17:16	Reserved
15	**Controller Running (CR)** — RO. When this bit is set, the DMA engines for a port are running.
14	**FIS Receive Running (FR)** — RO. When set, the FIS Receive DMA engine for the port is running.
13	**Mechanical Presence Switch State (MPSS)** — RO. The MPSS bit reports the state of a mechanical presence switch attached to this port. If CAP.SMPS is set to 1 and the mechanical presence switch is closed then this bit is cleared to 0. If CAP.SMPS is set to 1 and the mechanical presence switch is open then this bit is set to 1. If CAP.SMPS is set to '0' then this bit is cleared to 0. Software should only use this bit if both CAP.SMPS and PxCMD.MPSP are set to 1.

Bit	Description
12:8	**Current Command Slot (CCS)** — RO**.** Indicates the current command slot Intel® Xeon® Processor D-1500 Product Family is processing. This field is valid when the ST bit is set in this register, and is constantly updated by Intel® Xeon® Processor D-1500 Product Family. This field can be updated as soon as Intel® Xeon® Processor D-1500 Product Family recognizes an active command slot, or at some point soon after when it begins processing the command. This field is used by software to determine the current command issue location of Intel® Xeon® Processor D-1500 Product Family. In queued mode, software shall not use this field, as its value does not represent the current command being executed. Software shall only use PxCI and PxSACT when running queued commands.
7:5	Reserved
4	**FIS Receive Enable (FRE)** — R/W. When set, Intel® Xeon® Processor D-1500 Product Family may post received FISes into the FIS receive area pointed to by PxFB (ABAR+108h/188h/208h/288h) and PxFBU (ABAR+10Ch/18Ch/20Ch/28Ch). When cleared, received FISes are not accepted by Intel® Xeon® Processor D-1500 Product Family, except for the first D2H (device-to-host) register FIS after the initialization sequence. System software must not set this bit until PxFB (PxFBU) have been programmed with a valid pointer to the FIS receive area, and if software wishes to move the base, this bit must first be cleared, and software must wait for the FR bit (bit 14) in this register to be cleared.
3	**Command List Override (CLO)** — R/W. Setting this bit to 1 causes PxTFD.STS.BSY and PxTFD.STS.DRQ to be cleared to 0. This allows a software reset to be transmitted to the device regardless of whether the BSY and DRQ bits are still set in the PxTFD.STS register. The Controller sets this bit to 0 when PxTFD.STS.BSY and PxTFD.STS.DRQ have been cleared to 0. A write to this register with a value of 0 shall have no effect. This bit shall only be set to 1 immediately prior to setting the PxCMD.ST bit to 1 from a previous value of 0. Setting this bit to 1 at any other time is not supported and will result in indeterminate behavior. Software must wait for CLO to be cleared to 0 before setting PxCMD.ST to 1.
2	**Power On Device (POD)** — RO**.** Cold presence detect not supported. Defaults to 1.
1	**Spin-Up Device (SUD)** — R/W / RO This bit is R/W and defaults to 0 for systems that support staggered spin-up (R/W when CAP.SSS (ABAR+00h:bit 27) is 1). Bit is RO 1 for systems that do not support staggered spin-up (when CAP.SSS is 0). 0 = No action. 1 = On an edge detect from 0 to 1, Intel® Xeon® Processor D-1500 Product Family starts a COMRESET initialization sequence to the device. Clearing this bit to 0 does not cause any OOB signal to be sent on the interface. When this bit is cleared to 0 and PxSCTL.DET=0h, the controller will enter listen mode.
0	**Start (ST)** — R/W**.** When set, Intel® Xeon® Processor D-1500 Product Family may process the command list. When cleared, Intel® Xeon® Processor D-1500 Product Family may not process the command list. Whenever this bit is changed from a 0 to a 1, Intel® Xeon® Processor D-1500 Product Family starts processing the command list at entry 0. Whenever this bit is changed from a 1 to a 0, the PxCI register is cleared by Intel® Xeon® Processor D-1500 Product Family upon Intel® Xeon® Processor D-1500 Product Family putting the controller into an idle state. Refer to Section 10.3 of the *Serial ATA AHCI Specification* for important restrictions on when ST can be set to 1 and cleared to 0.

8.4.2.8 PxTFD—Port [5:0] Task File Data Register (D31:F2)

Address Offset: Port 0: ABAR + 120h — Attribute: RO
Port 1: ABAR + 1A0h
Port 2: ABAR + 220h (if port available; see Section 1.3)
Port 3: ABAR + 2A0h (if port available; see Section 1.3)
Port 4: ABAR + 320h
Port 5: ABAR + 3A0h
Default Value: 0000007Fh — Size: 32 bits

This is a 32-bit register that copies specific fields of the task file when FISes are received. The FISes that contain this information are: D2H Register FIS,PIO Setup FIS and Set Device Bits FIS

Bit	Description
31:16	Reserved
15:8	**Error (ERR)** — RO**.** Contains the latest copy of the task file error register.

Bit	Description
7:0	**Status (STS)** — RO. Contains the latest copy of the task file status register. Fields in this register that affect AHCI. **Bit** / **Field** / **Definition** 7 / BSY / Indicates the interface is busy 6:4 / N/A / Not applicable 3 / DRQ / Indicates a data transfer is requested 2:1 / N/A / Not applicable 0 / ERR / Indicates an error during the transfer

8.4.2.9 PxSIG—Port [5:0] Signature Register (D31:F2)

Address Offset: Port 0: ABAR + 124h — Attribute: RO
Port 1: ABAR + 1A4h
Port 2: ABAR + 224h (if port available; see Section 1.3)
Port 3: ABAR + 2A4h (if port available; see Section 1.3)
Port 4: ABAR + 324h
Port 5: ABAR + 3A4h
Default Value: FFFFFFFFh — Size: 32 bits

This is a 32-bit register which contains the initial signature of an attached device when the first D2H Register FIS is received from that device. It is updated once after a reset sequence.

Bit	Description
31:0	**Signature (SIG)** — RO. Contains the signature received from a device on the first D2H register FIS. The bit order is as follows: **Bit** / **Field** 31:24 / LBA High Register 23:16 / LBA Mid Register 15:8 / LBA Low Register 7:0 / Sector Count Register

8.4.2.10 PxSSTS—Port [5:0] Serial ATA Status Register (D31:F2)

Address Offset: Port 0: ABAR + 128h — Attribute: RO
Port 1: ABAR + 1A8h
Port 2: ABAR + 228h (if port available; see Section 1.3)
Port 3: ABAR + 2A8h (if port available; see Section 1.3)
Port 4: ABAR + 328h
Port 5: ABAR + 3A8h
Default Value: 00000000h — Size: 32 bits

This is a 32-bit register that conveys the current state of the interface and host. Intel® Xeon® Processor D-1500 Product Family updates it continuously and asynchronously. When Intel® Xeon® Processor D-1500 Product Family transmits a COMRESET to the device, this register is updated to its reset values.

Bit	Description
31:12	Reserved

Bit	Description
11:8	**Interface Power Management (IPM)** — RO**.** Indicates the current interface state: **Value** — **Description** 0h — Device not present or communication not established 1h — Interface in active state 2h — Interface in PARTIAL power management state 6h — Interface in SLUMBER power management state All other values reserved.
7:4	**Current Interface Speed (SPD)** — RO. Indicates the negotiated interface communication speed. **Value** — **Description** 0h — Device not present or communication not established 1h — Generation 1 communication rate negotiated 2h — Generation 2 communication rate negotiated 3h — Generation 3 communication rate negotiated All other values reserved. Intel® Xeon® Processor D-1500 Product Family supports Gen 1 communication rates (1.5 Gb/s), Gen 2 rates (3.0 Gb/s) and Gen 3 rates (6.0 Gb/s)
3:0	**Device Detection (DET)** — RO**.** Indicates the interface device detection and Phy state: **Value** — **Description** 0h — No device detected and Phy communication not established 1h — Device presence detected but Phy communication not established 3h — Device presence detected and Phy communication established 4h — Phy in offline mode as a result of the interface being disabled or running in a BIST loopback mode All other values reserved.

8.4.2.11 PxSCTL — Port [5:0] Serial ATA Control Register (D31:F2)

Address Offset:	Port 0: ABAR + 12Ch Port 1: ABAR + 1ACh Port 2: ABAR + 22Ch (if port available; see Section 1.3) Port 3: ABAR + 2ACh (if port available; see Section 1.3) Port 4: ABAR + 32Ch Port 5: ABAR + 3ACh	Attribute:	R/W, RO
Default Value:	00000004h	Size:	32 bits

This is a 32-bit read-write register by which software controls SATA capabilities. Writes to the SControl register result in an action being taken by Intel® Xeon® Processor D-1500 Product Family or the interface. Reads from the register return the last value written to it.

Bit	Description
31:20	Reserved
19:16	**Port Multiplier Port (PMP)** — R/W. This field is not used by AHCI
15:12	**Select Power Management (SPM)** — R/W. This field is not used by AHCI

Bit	Description
11:8	**Interface Power Management Transitions Allowed (IPM)** — R/W**.** Indicates which power states Intel® Xeon® Processor D-1500 Product Family is allowed to transition to: **Value** — **Description** 0h — No interface restrictions 1h — Transitions to the PARTIAL state disabled 2h — Transitions to the SLUMBER state disabled 3h — Transitions to both PARTIAL and SLUMBER states disabled All other values reserved
7:4	**Speed Allowed (SPD)** — R/W. Indicates the highest allowable speed of the interface. This speed is limited by the CAP.ISS (ABAR+00h:bit 23:20) field. **Value** — **Description** 0h — No speed negotiation restrictions 1h — Limit speed negotiation to Generation 1 communication rate 2h — Limit speed negotiation to Generation 2 communication rate 3h — Limit speed negotiation to Generation 3 communication rate Intel® Xeon® Processor D-1500 Product Family Supports Gen 1 communication rates (1.5 Gb/s), Gen 2 rates (3.0 Gb/s) and Gen 3 rates (6.0 Gb/s). If software changes SPD after port has been enabled, software is required to perform a port reset using DET=1h. This field shall remain 1h until set to another value by software.
3:0	**Device Detection Initialization (DET)** — R/W. Controls Intel® Xeon® Processor D-1500 Product Family's device detection and interface initialization. **Value** — **Description** 0h — No device detection or initialization action requested 1h — Perform interface communication initialization sequence to establish communication. This is functionally equivalent to a hard reset and results in the interface being reset and communications re-initialized 4h — Disable the Serial ATA interface and put Phy in offline mode All other values reserved. When this field is written to a 1h, Intel® Xeon® Processor D-1500 Product Family initiates COMRESET and starts the initialization process. When the initialization is complete, this field shall remain 1h until set to another value by software. This field may only be changed to 1h or 4h when PxCMD.ST is 0. Changing this field while Intel® Xeon® Processor D-1500 Product Family is running results in undefined behavior. ***Note:*** It is permissible to implement any of the Serial ATA defined behaviors for transmission of COMRESET when DET=1h.

8.4.2.12 PxSERR—Port [5:0] Serial ATA Error Register (D31:F2)

Address Offset: Port 0: ABAR + 130h — Attribute: R/WC
Port 1: ABAR + 1B0h
Port 2: ABAR + 230h (if port available; see Section 1.3)
Port 3: ABAR + 2B0h (if port available; see Section 1.3)
Port 4: ABAR + 330h
Port 5: ABAR + 3B0h
Default Value: 00000000h — Size: 32 bits

Bits 26:16 of this register contain diagnostic error information for use by diagnostic software in validating correct operation or isolating failure modes. Bits 11:0 contain error information used by host software in determining the appropriate response to the error condition. If one or more of bits 11:8 of this register are set, the controller will stop the current transfer.

Bit	Description
31:27	Reserved
26	**Exchanged (X)** — R/WC. When set to 1, this bit indicates that a change in device presence has been detected since the last time this bit was cleared. This bit shall always be set to 1 anytime a COMINIT signal is received. This bit is reflected in the P0IS.PCS bit.
25	**Unrecognized FIS Type (F)** — R/WC. Indicates that one or more FISs were received by the Transport layer with good CRC, but had a type field that was not recognized.
24	**Transport state transition error (T)** — R/WC. Indicates that an error has occurred in the transition from one state to another within the Transport layer since the last time this bit was cleared.
23	**Link Sequence Error (S):** Indicates that one or more Link state machine error conditions was encountered. The Link Layer state machine defines the conditions under which the link layer detects an erroneous transition.
22	**Handshake (H)** — R/WC. Indicates that one or more R_ERR handshake response was received in response to frame transmission. Such errors may be the result of a CRC error detected by the recipient, a disparity or 8b/10b decoding error, or other error condition leading to a negative handshake on a transmitted frame.
21	**CRC Error (C)** — R/WC. Indicates that one or more CRC errors occurred with the Link Layer.
20	**Disparity Error (D)** — R/WC. This field is not used by AHCI.
19	**10b to 8b Decode Error (B)** — R/WC. Indicates that one or more 10b to 8b decoding errors occurred.
18	**Comm Wake (W)** — R/WC. Indicates that a Comm Wake signal was detected by the Phy.
17	**Phy Internal Error (I)** — R/WC. Indicates that the Phy detected some internal error.
16	**PhyRdy Change (N)** — R/WC. When set to 1, this bit indicates that the internal PhyRdy signal changed state since the last time this bit was cleared. In Intel® Xeon® Processor D-1500 Product Family, this bit will be set when PhyRdy changes from a 0 -> 1 or a 1 -> 0. The state of this bit is then reflected in the PxIS.PRCS interrupt status bit and an interrupt will be generated if enabled. Software clears this bit by writing a 1 to it.
15:12	Reserved
11	**Internal Error (E)** — R/WC. The SATA controller failed due to a master or target abort when attempting to access system memory.
10	**Protocol Error (P)** — R/WC. A violation of the Serial ATA protocol was detected. ***Note:*** Intel® Xeon® Processor D-1500 Product Family does not set this bit for all protocol violations that may occur on the SATA link.
9	**Persistent Communication or Data Integrity Error (C)** — R/WC. A communication error that was not recovered occurred that is expected to be persistent. Persistent communications errors may arise from faulty interconnect with the device, from a device that has been removed or has failed, or a number of other causes.
8	**Transient Data Integrity Error (T)** — R/WC. A data integrity error occurred that was not recovered by the interface.
7:2	Reserved.
1	**Recovered Communications Error (M)** — R/WC. Communications between the device and host was temporarily lost but was re-established. This can arise from a device temporarily being removed, from a temporary loss of Phy synchronization, or from other causes and may be derived from the PhyNRdy signal between the Phy and Link layers.
0	**Recovered Data Integrity Error (I)** — R/WC. A data integrity error occurred that was recovered by the interface through a retry operation or other recovery action.

8.4.2.13 PxSACT—Port [5:0] Serial ATA Active Register (D31:F2)

Address Offset: Port 0: ABAR + 134h — Attribute: R/W
Port 1: ABAR + 1B4h
Port 2: ABAR + 234h (if port available; see Section 1.3)
Port 3: ABAR + 2B4h (if port available; see Section 1.3)
Port 4: ABAR + 334h
Port 5: ABAR + 3B4h
Default Value: 00000000h — Size: 32 bits

Bit	Description
31:0	**Device Status (DS)** — R/W. System software sets this bit for SATA queuing operations prior to setting the PxCI.CI bit in the same command slot entry. This field is cleared using the Set Device Bits FIS. This field is also cleared when PxCMD.ST (ABAR+118h/198h/218h/298h:bit 0) is cleared by software, and as a result of a COMRESET or SRST.

8.4.2.14 PxCI—Port [5:0] Command Issue Register (D31:F2)

Address Offset: Port 0: ABAR + 138h — Attribute: R/W
Port 1: ABAR + 1B8h
Port 2: ABAR + 238h (if port available; see Section 1.3)
Port 3: ABAR + 2B8h (if port available; see Section 1.3)
Port 4: ABAR + 338h
Port 5: ABAR + 3B8h
Default Value: 00000000h — Size: 32 bits

Bit	Description
31:0	**Commands Issued (CI)** — R/W. This field is set by software to indicate to Intel® Xeon® Processor D-1500 Product Family that a command has been built-in system memory for a command slot and may be sent to the device. When Intel® Xeon® Processor D-1500 Product Family receives a FIS which clears the BSY and DRQ bits for the command, it clears the corresponding bit in this register for that command slot. Bits in this field shall only be set to 1 by software when PxCMD.ST is set to 1. This field is also cleared when PxCMD.ST (ABAR+118h/198h/218h/298h:bit 0) is cleared by software.

§

9 SATA Controller Registers (D31:F5)

9.1 PCI Configuration Registers (SATA–D31:F5)

Note: Address locations that are not shown should be treated as Reserved.

All of the SATA registers are in the core well. None of the registers can be locked.

Table 9-1. SATA Controller PCI Register Address Map (SATA–D31:F5) (Sheet 1 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
00h–01h	VID	Vendor Identification	8086h	RO
02h–03h	DID	Device Identification	See register description	RO
04h–05h	PCICMD	PCI Command	0000h	R/W, RO
06h–07h	PCISTS	PCI Status	02B0h	R/WC, RO
08h	RID	Revision Identification	See register description	RO
09h	PI	Programming Interface	See register description	See register description
0Ah	SCC	Sub Class Code	See register description	See register description
0Bh	BCC	Base Class Code	01h	RO
10h–13h	PCMD_BAR	Primary Command Block Base Address	00000001h	R/W, RO
14h–17h	PCNL_BAR	Primary Control Block Base Address	00000001h	R/W, RO
18h–1Bh	SCMD_BAR	Secondary Command Block Base Address	00000001h	R/W, RO
1Ch–1Fh	SCNL_BAR	Secondary Control Block Base Address	00000001h	R/W, RO
20h–23h	BAR	Legacy Bus Master Base Address	00000001h	R/W, RO
24h–27h	SIDPBA	Serial ATA Index / Data Pair Base Address	00000000h	See register description
2Ch–2Dh	SVID	Subsystem Vendor Identification	0000h	R/WO
2Eh–2Fh	SID	Subsystem Identification	0000h	R/WO
34h	CAP	Capabilities Pointer	80h	RO
3Ch	INT_LN	Interrupt Line	00h	R/W
3Dh	INT_PN	Interrupt Pin	See register description	RO
40h–41h	IDE_TIM	Primary IDE Timing	0000h	R/W
42h–43h	IDE_TIM	Secondary IDE Timing	0000h	R/W
44h	SIDETIM	Slave IDE Timing	00h	R/W
48h	SDMA_CNT	Synchronous DMA Control	00h	R/W
4Ah–4Bh	SDMA_TIM	Synchronous DMA Timing	0000h	R/W
54h–57h	IDE_CONFIG	IDE I/O Configuration	00000000h	R/W
70h–71h	PID	PCI Power Management Capability Identification	See register description	RO
72h–73h	PC	PCI Power Management Capabilities	4003h	RO
74h–75h	PMCS	PCI Power Management Control and Status	0008h	R/W, RO, R/WC

Table 9-1. SATA Controller PCI Register Address Map (SATA–D31:F5) (Sheet 2 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
90h–91h	MAP	Address Map	0000h	R/W
92h–93h	PCS	Port Control and Status	0000h	R/W, RO, R/WC
A8h–ABh	SATACR0	SATA Capability Register 0	0010B012h	RO, R/WO
ACh–AFh	SATACR1	SATA Capability Register 1	00000048h	RO
B0h–B1h	FLRCID	FLR Capability ID	0009h	RO
B2h–B3h	FLRCLV	FLR Capability Length and Value	2006h	RO
B4h–B5h	FLRCTRL	FLR Control	0000h	R/W, RO
C0h	ATC	APM Trapping Control	00h	R/W
C4h	ATS	APM Trapping Status	00h	R/WC

Note: Intel® Xeon® Processor D-1500 Product Family SATA controller is not arbitrated as a PCI device; therefore, it does not need a master latency timer.

9.1.1 VID—Vendor Identification Register (SATA—D31:F5)

Offset Address: 00h–01h
Default Value: 8086h
Lockable: No
Attribute: RO
Size: 16 bit
Power Well: Core

Bit	Description
15:0	**Vendor ID** — RO. This is a 16-bit value assigned to Intel. Intel VID = 8086h

9.1.2 DID—Device Identification Register (SATA—D31:F5)

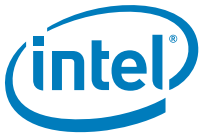
Offset Address: 02h–03h
Default Value: See bit description
Lockable: No
Attribute: RO
Size: 16 bit
Power Well: Core

Bit	Description
15:0	**Device ID** — RO. This is a 16-bit value assigned to Intel® Xeon® Processor D-1500 Product Family SATA controller. ***Note:*** The value of this field will change dependent upon the value of the MAP Register.

9.1.3 PCICMD—PCI Command Register (SATA–D31:F5)

Address Offset: 04h–05h
Default Value: 0000h
Attribute: RO, R/W
Size: 16 bits

Bit	Description
15:11	Reserved
10	**Interrupt Disable** — R/W. This disables pin-based INTx# interrupts. This bit has no effect on MSI operation. 0 = Internal INTx# messages are generated if there is an interrupt and MSI is not enabled. 1 = Internal INTx# messages will not be generated.
9	Fast Back to Back Enable (FBE) — RO. Hardwired to 0.
8	SERR# Enable **(SERR_EN)** — RO. Hardwired to 0.
7	Wait Cycle Control (WCC) — RO. Hardwired to 0.
6	**Parity Error Response (PER)** — R/W. 0 = Disabled. SATA controller will not generate PERR# when a data parity error is detected. 1 = Enabled. SATA controller will generate PERR# when a data parity error is detected.



Bit	Description
5	VGA Palette Snoop (VPS) — RO. Hardwired to 0.
4	Postable Memory Write Enable (PMWE) — RO. Hardwired to 0.
3	Special Cycle Enable (SCE) — RO. Hardwired to 0.
2	**Bus Master Enable (BME)** — R/W. This bit controls Intel® Xeon® Processor D-1500 Product Family ability to act as a PCI master for IDE Bus Master transfers. This bit does not impact the generation of completions for split transaction commands.
1	**Memory Space Enable (MSE)** — RO. This controller does not support AHCI; therefore, no memory space is required.
0	**I/O Space Enable (IOSE)** — R/W. This bit controls access to the I/O space registers. 0 = Disables access to the Legacy or Native IDE ports (both Primary and Secondary) as well as the Bus Master I/O registers. 1 = Enable. The Base Address register for the Bus Master registers should be programmed before this bit is set.

9.1.4 PCISTS — PCI Status Register (SATA–D31:F5)

Address Offset: 06h–07h
Attribute: R/WC, RO
Default Value: 02B0h
Size: 16 bits

Note: For the writable bits, software must write a 1 to clear bits that are set. Writing a 0 to the bit has no effect.

Bit	Description
15	**Detected Parity Error (DPE)** — R/WC. 0 = No parity error detected by SATA controller. 1 = SATA controller detects a parity error on its interface.
14	Signaled System Error (SSE) — RO. Hardwired to 0.
13	**Received Master Abort (RMA)** — R/WC. 0 = Master abort Not generated. 1 = SATA controller, as a master, generated a master abort.
12	Reserved
11	Signaled Target Abort (STA) — RO. Hardwired to 0.
10:9	**DEVSEL# Timing Status (DEV_STS)** — RO. 01 = Hardwired; Controls the device select time for the SATA controller's PCI interface.
8	**Data Parity Error Detected (DPED)** — R/WC. For Intel® Xeon® Processor D-1500 Product Family, this bit can only be set on read completions received from SiBUS where there is a parity error. 1 = SATA controller, as a master, either detects a parity error or sees the parity error line asserted, and the parity error response bit (bit 6 of the command register) is set.
7	Fast Back to Back Capable (FB2BC) — RO. Hardwired to 1.
6	User Definable Features (UDF) — RO. Hardwired to 0.
5	66 MHz Capable (66MHZ_CAP) — RO. Hardwired to 1.
4	**Capabilities List (CAP_LIST)** — RO. This bit indicates the presence of a capabilities list. The minimum requirement for the capabilities list must be PCI power management for the SATA controller.
3	**Interrupt Status (INTS)** — RO. Reflects the state of INTx# messages, IRQ14 or IRQ15. 0 = Interrupt is cleared (independent of the state of Interrupt Disable bit in the command register [offset 04h]). 1 = Interrupt is to be asserted
2:0	Reserved

9.1.5 RID—Revision Identification Register (SATA—D31:F5)

Offset Address: 08h | Attribute: RO
Default Value: See bit description | Size: 8 bits

Bit	Description
7:0	**Revision ID** — RO. This field indicates the device specific revision identifier.

9.1.6 PI—Programming Interface Register (SATA–D31:F5)

Address Offset: 09h | Attribute: RO
Default Value: 85h | Size: 8 bits

When SCC = 01h

Bit	Description
7	This read-only bit is a 1 to indicate that Intel® Xeon® Processor D-1500 Product Family supports bus master operation
6:4	Reserved
3	**Secondary Mode Native Capable (SNC)** — RO. Indicates whether or not the secondary channel has a fixed mode of operation. 0 = Indicates the mode is fixed and is determined by the (read-only) value of bit 2. This bit will always return 0.
2	**Secondary Mode Native Enable (SNE)** — RO. Determines the mode that the secondary channel is operating in. 1 = Secondary controller operating in native PCI mode. This bit will always return 1.
1	**Primary Mode Native Capable (PNC)** — RO. Indicates whether or not the primary channel has a fixed mode of operation. 0 = Indicates the mode is fixed and is determined by the (read-only) value of bit 0. This bit will always return 0.
0	**Primary Mode Native Enable (PNE)** — RO. Determines the mode that the primary channel is operating in. 1 = Primary controller operating in native PCI mode. This bit will always return 1.

9.1.7 SCC—Sub Class Code Register (SATA–D31:F5)

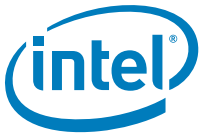
Address Offset: 0Ah | Attribute: RO
Default Value: 01h | Size: 8 bits

Bit	Description
7:0	**Sub Class Code (SCC)** — RO. The value of this field determines whether the controller supports legacy IDE mode.

9.1.8 BCC—Base Class Code Register (SATA–D31:F5SATA–D31:F5)

Address Offset: 0Bh | Attribute: RO
Default Value: 01h | Size: 8 bits

Bit	Description
7:0	**Base Class Code (BCC)** — RO. 01h = Mass storage device



9.1.9 PCMD_BAR—Primary Command Block Base Address Register (SATA–D31:F5)

Address Offset: 10h–13h
Default Value: 00000001h
Attribute: R/W, RO
Size: 32 bits

Bit	Description
31:16	Reserved
15:3	**Base Address** — R/W. This field provides the base address of the I/O space (8 consecutive I/O locations).
2:1	Reserved
0	**Resource Type Indicator (RTE)** — RO. Hardwired to 1 to indicate a request for I/O space.

Note: This 8-byte I/O space is used in native mode for the Primary Controller's Command Block.

9.1.10 PCNL_BAR—Primary Control Block Base Address Register (SATA–D31:F5)

Address Offset: 14h–17h
Default Value: 00000001h
Attribute: R/W, RO
Size: 32 bits

Bit	Description
31:16	Reserved
15:2	**Base Address** — R/W. This field provides the base address of the I/O space (4 consecutive I/O locations).
1	Reserved
0	**Resource Type Indicator (RTE)** — RO. Hardwired to 1 to indicate a request for I/O space.

Note: This 4-byte I/O space is used in native mode for the Primary Controller's Command Block.

9.1.11 SCMD_BAR—Secondary Command Block Base Address Register (SATA D31:F5)

Address Offset: 18h–1Bh
Default Value: 00000001h
Attribute: R/W, RO
Size: 32 bits

Bit	Description
31:16	Reserved
15:3	**Base Address** — R/W. This field provides the base address of the I/O space (8 consecutive I/O locations).
2:1	Reserved
0	**Resource Type Indicator (RTE)** — RO. Hardwired to 1 to indicate a request for I/O space.

Note: This 8-byte I/O space is used in native mode for the Secondary Controller's Command Block.

9.1.12 SCNL_BAR—Secondary Control Block Base Address Register (SATA D31:F5)

Address Offset:	1Ch–1Fh	Attribute:	R/W, RO
Default Value:	00000001h	Size:	32 bits

Bit	Description
31:16	Reserved
15:2	**Base Address** — R/W. This field provides the base address of the I/O space (4 consecutive I/O locations).
1	Reserved
0	**Resource Type Indicator (RTE)** — RO. Hardwired to 1 to indicate a request for I/O space.

Note: This 4-byte I/O space is used in native mode for the Secondary Controller's Command Block.

9.1.13 BAR — Legacy Bus Master Base Address Register (SATA–D31:F5)

Address Offset:	20h–23h	Attribute:	R/W, RO
Default Value:	00000001h	Size:	32 bits

The Bus Master IDE interface function uses Base Address register 5 to request a 16-byte I/O space to provide a software interface to the Bus Master functions. Only 12 bytes are actually used (6 bytes for primary, 6 bytes for secondary). Only bits [15:4] are used to decode the address.

Bit	Description
31:16	Reserved
15:5	**Base Address** — R/W. This field provides the base address of the I/O space (16 consecutive I/O locations).
4	**Base Address 4 (BA4)**— R/W. When SCC is 01h, this bit will be R/W resulting in requesting 16B of I/O space.
3:1	Reserved
0	**Resource Type Indicator (RTE)** — RO. Hardwired to 1 to indicate a request for I/O space.

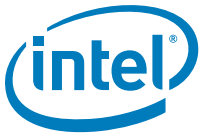
9.1.14 SIDPBA — SATA Index/Data Pair Base Address Register (SATA–D31:F5)

Address Offset:	24h–27h	Attribute:	R/W, RO
Default Value:	00000000h	Size:	32 bits

When SCC is 01h

When the programming interface is IDE, the register represents an I/O BAR allocating 16B of I/O space for the I/O mapped registers defined in Section 9.3. While 16B of locations are allocated, some maybe reserved.

Bit	Description
31:16	Reserved
15:4	**Base Address (BA)** — R/W. Base address of register I/O space
3:1	Reserved
0	**Resource Type Indicator (RTE)** — RO. Hardwired to 1 to indicate a request for I/O space.



9.1.15 SVID—Subsystem Vendor Identification Register (SATA–D31:F5)

Address Offset: 2Ch–2Dh
Default Value: 0000h
Lockable: No
Function Level Reset:No
Attribute: R/WO
Size: 16 bits
Power Well: Core

Bit	Description
15:0	**Subsystem Vendor ID (SVID)** — R/WO. Value is written by BIOS. No hardware action taken on this value.

9.1.16 SID—Subsystem Identification Register (SATA–D31:F5)

Address Offset: 2Eh–2Fh
Default Value: 0000h
Lockable: No
Attribute: R/WO
Size: 16 bits
Power Well: Core

Bit	Description
15:0	**Subsystem ID (SID)** — R/WO. Value is written by BIOS. No hardware action taken on this value.

9.1.17 CAP—Capabilities Pointer Register (SATA–D31:F5)

Address Offset: 34h
Default Value: 70h
Attribute: RO
Size: 8 bits

Bit	Description
7:0	**Capabilities Pointer (CAP_PTR)** — RO. Indicates that the first capability pointer offset is 70h if the Sub Class Code (SCC) (Dev 31:F2:0Ah) is configure as IDE mode (value of 01).

9.1.18 INT_LN—Interrupt Line Register (SATA–D31:F5)

Address Offset: 3Ch
Default Value: 00h
Function Level Reset: No
Attribute: R/W
Size: 8 bits

Bit	Description
7:0	**Interrupt Line** — R/W. This field is used to communicate to software the interrupt line that the interrupt pin is connected to. These bits are not reset by FLR.

9.1.19 INT_PN—Interrupt Pin Register (SATA–D31:F5)

Address Offset: 3Dh
Default Value: See Register Description
Attribute: RO
Size: 8 bits

Bit	Description
7:0	**Interrupt Pin** — RO. This reflects the value of D31IP.SIP1 (Chipset Config Registers:Offset 3100h:bits 11:8).

9.1.20 IDE_TIM—IDE Timing Register (SATA–D31:F5)

Address Offset: Primary: 40h–41h
Secondary: 42h–43h
Attribute: R/W
Default Value: 0000h
Size: 16 bits

Bits 14:12 and 9:0 of this register are R/W to maintain software compatibility. These bits have no effect on hardware.

Bit	Description
15	**IDE Decode Enable (IDE)** — R/W. Individually enable/disable the Primary or Secondary decode. 0 = Disable. 1 = Enables Intel® Xeon® Processor D-1500 Product Family to decode the associated Command Block and Control Block.
14:12	**IDE_TIM Field 2** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.
11:10	Reserved
9:0	**IDE_TIM Field 1** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.

9.1.21 SDMA_CNT—Synchronous DMA Control Register (SATA–D31:F5)

Address Offset: 48h
Attribute: R/W
Default Value: 00h
Size: 8 bits

Note: This register is R/W to maintain software compatibility. These bits have no effect on hardware.

Bit	Description
7:3	Reserved
2	**Secondary Master ATAxx Enable (SDAE0)** — R/W. 0 = Disable (default) 1 = Enable DMA timing modes for the secondary master device.
1	Reserved
0	**Primary Master ATAxx Enable (PDAE0)** — R/W. 0 = Disable (default) 1 = Enable DMA timing modes for the primary master device

9.1.22 SDMA_TIM—Synchronous DMA Timing Register (SATA–D31:F5)

Address Offset: 4Ah–4Bh
Attribute: R/W
Default Value: 0000h
Size: 16 bits

Note: This register is R/W to maintain software compatibility. These bits have no effect on hardware.

Bit	Description
15:10	Reserved
9:8	**SDMA_TIM Field 2**— R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.
7:2	Reserved
1:0	**SDMA_TIM Field 1** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.

9.1.23 IDE_CONFIG—IDE I/O Configuration Register (SATA–D31:F5)

Address Offset: 54h–57h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits

Note: This register is R/W to maintain software compatibility. These bits have no effect on hardware.

Bit	Description
31:24	Reserved
23:16	**IDE_CONFIG Field 6** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.
15	Reserved
14	**IDE_CONFIG Field 5** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.
13	Reserved
12	**IDE_CONFIG Field 4** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.
11:8	Reserved
7:4	**IDE_CONFIG Field 3** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.
3	Reserved
2	**IDE_CONFIG Field 2** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.
1	Reserved
0	**IDE_CONFIG Field 1** — R/W. This field is R/W to maintain software compatibility. This field has no effect on hardware.

9.1.24 PID—PCI Power Management Capability Identification Register (SATA–D31:F5)

Address Offset: 70h–71h
Default Value: B001h
Attribute: RO
Size: 16 bits

Bits	Description
15:8	**Next Capability (NEXT)** — RO. When SCC is 01h, this field will be B0h indicating the next item is FLR Capability Pointer in the list.
7:0	**Capability ID (CID)** — RO. Indicates that this pointer is a PCI power management.

9.1.25 PC—PCI Power Management Capabilities Register (SATA–D31:F5)

Address Offset: 72h–73h
Default Value: 4003h
Attribute: RO
Size: 16 bits

Bits	Description
15:11	**PME Support (PME_SUP)** — RO. By default with SCC = 01h, the default value of 00000 indicates no PME support in IDE mode.
10	D2 Support (D2_SUP) — RO. Hardwired to 0. The D2 state is not supported
9	D1 Support (D1_SUP) — RO. Hardwired to 0. The D1 state is not supported
8:6	Auxiliary Current (AUX_CUR) — RO. PME# from D3COLD state is not supported, therefore this field is 000b.

Bits	Description
5	Device Specific Initialization (DSI) — RO. Hardwired to 0 to indicate that no device-specific initialization is required.
4	Reserved
3	PME Clock (PME_CLK) — RO. Hardwired to 0 to indicate that PCI clock is not required to generate PME#.
2:0	**Version (VER)** — RO. Hardwired to 011 to indicates support for Revision 1.2 of the PCI Power Management Specification.

9.1.26 PMCS—PCI Power Management Control and Status Register (SATA–D31:F5)

Address Offset: 74h–75h
Attribute: RO, R/W, R/WC
Default Value: 0008h
Size: 16 bits
Function Level Reset: No (Bits 8 and 15 only)

Bits	Description
15	**PME Status (PMES)** — R/WC. Bit is set when a PME event is to be requested, and if this bit and PMEE is set, a PME# will be generated from the SATA controller. ***Note:*** When SCC=01h this bit will be RO 0. Software is advised to clear PMEE together with PMES prior to changing SCC through MAP.SMS. This bit is not reset by Function Level Reset.
14:9	Reserved
8	**PME Enable (PMEE)** — R/W. When SCC is not 01h, this bit R/W. When set, the SATA controller generates PME# form $D3_{HOT}$ on a wake event. ***Note:*** When SCC=01h, this bit will be RO 0. Software is advised to clear PMEE together with PMES prior to changing SCC through MAP.SMS. This bit is not reset by Function Level Reset.
7:4	Reserved
3	**No Soft Reset (NSFRST)** — RO. These bits are used to indicate whether devices transitioning from $D3_{HOT}$ state to D0 state will perform an internal reset. 0 = Device transitioning from $D3_{HOT}$ state to D0 state perform an internal reset. 1 = Device transitioning from $D3_{HOT}$ state to D0 state do not perform an internal reset. Configuration content is preserved. Upon transition from the $D3_{HOT}$ state to D0 state initialized state, no additional operating system intervention is required to preserve configuration context beyond writing to the PowerState bits. Regardless of this bit, the controller transition from $D3_{HOT}$ state to D0 state by a system or bus segment reset will return to the state D0 uninitialized with only PME context preserved if PME is supported and enabled.
2	Reserved
1:0	**Power State (PS)** — R/W. These bits are used both to determine the current power state of the SATA controller and to set a new power state. 00 = D0 state 11 = $D3_{HOT}$ state When in the $D3_{HOT}$ state, the controller's configuration space is available, but the I/O and memory spaces are not. Additionally, interrupts are blocked.

9.1.27 MAP—Address Map Register (SATA–D31:F5)

Address Offset: 90h–91h
Attribute: R/W, R/WO, RO
Default Value: 0000h
Size: bits
Function Level Reset: No (Bits 9:8 only)

Bits	Description
15:8	Reserved
7:6	**SATA Mode Select (SMS)** — R/W. Software programs these bits to control the mode in which the SATA Controller should operate. 00b = IDE Mode All other combinations are reserved.
5:2	Reserved
1:0	**Map Value (MV)**— Reserved.

9.1.28 PCS—Port Control and Status Register (SATA–D31:F5)

Address Offset: 92h–93h
Attribute: R/W, RO
Default Value: 0000h
Size: 16 bits
Function Level Reset: No

By default, the SATA ports are set to the disabled state (bits [5:0] = 0). When enabled by software, the ports can transition between the on, partial, and slumber states and can detect devices. When disabled, the port is in the "off" state and cannot detect any devices.

If an AHCI-aware or RAID enabled operating system is being booted, then system BIOS shall insure that all supported SATA ports are enabled prior to passing control to the OS. Once the AHCI aware OS is booted, it becomes the enabling/disabling policy owner for the individual SATA ports. This is accomplished by manipulating a port PxSCTL and PxCMD fields. Because an AHCI or RAID aware OS will typically not have knowledge of the PxE bits and because the PxE bits act as master on/off switches for the ports, pre-boot software must insure that these bits are set to 1 prior to booting the OS, regardless as to whether or not a device is currently on the port.

Bits	Description
15:10	Reserved
9	**Port 5 Present (P5P)** — RO. The status of this bit may change at any time. This bit is cleared when the port is disabled using P1E. This bit is not cleared upon surprise removal of a device. 0 = No device detected. 1 = The presence of a device on Port 1 has been detected.
8	**Port 4 Present (P4P)** — RO. The status of this bit may change at any time. This bit is cleared when the port is disabled using P0E. This bit is not cleared upon surprise removal of a device. 0 = No device detected. 1 = The presence of a device on Port 0 has been detected.
7:2	Reserved
1	**Port 5 Enabled (P5E)** — R/W. 0 = Disabled. The port is in the 'off' state and cannot detect any devices. 1 = Enabled. The port can transition between the on, partial, and slumber states and can detect devices. This bit is read-only 0 when MAP.SPD[1]= 1 pr is a PCIe Port.

Bits	Description
0	**Port 4 Enabled (P4E)** — R/W. 0 = Disabled. The port is in the 'off' state and cannot detect any devices. 1 = Enabled. The port can transition between the on, partial, and slumber states and can detect devices. This bit is read-only 0 when MAP.SPD[0]= 1 or is a PCIe Port.

9.1.29 SATACR0—SATA Capability Register 0 (SATA–D31:F5)

Address Offset: A8h–ABh Attribute: RO, R/WO
Default Value: 0010B012h Size: 32 bits
Function Level Reset: No (Bits 15:8 only)

When SCC is 01h, this register is read-only 0.

Bit	Description
31:24	Reserved
23:20	**Major Revision (MAJREV)** — RO. Major revision number of the SATA Capability Pointer implemented.
19:16	**Minor Revision (MINREV)** — RO. Minor revision number of the SATA Capability Pointer implemented.
15:8	**Next Capability Pointer (NEXT)** — R/WO. Points to the next capability structure.
7:0	**Capability ID (CAP)** — RO. The value of 12h has been assigned by the PCI SIG to designate the SATA capability pointer.

9.1.30 SATACR1—SATA Capability Register 1 (SATA–D31:F5)

Address Offset: ACh–AFh Attribute: RO
Default Value: 00000048h Size: 32 bits

When SCC is 01h, this register is read-only 0.

Bit	Description
31:16	Reserved
15:4	**BAR Offset (BAROFST)** — RO. Indicates the offset into the BAR where the index/Data pair are located (in DWord granularity). The index and Data I/O registers are located at offset 10h within the I/O space defined by LBAR (BAR4). A value of 004h indicates offset 10h.
3:0	**BAR Location (BARLOC)** — RO. Indicates the absolute PCI Configuration Register address of the BAR containing the Index/Data pair (in DWord granularity). The Index and Data I/O registers reside within the space defined by LBAR (BAR4) in the SATA controller. a value of 8h indicates and offset of 20h, which is LBAR (BAR4).

9.1.31 FLRCID—FLR Capability ID Register (SATA–D31:F5)

Address Offset: B0h–B1h Attribute: RO
Default Value: 0009h Size: 16 bits

Bit	Description
15:8	**Next Capability Pointer** — RO. A value of 00h indicates the final item in the Capability List.
7:0	**Capability ID** — RO. The value of this field depends on the FLRCSSECL bit. If FLRCSSEL = 0, this field is 13h If FLRCSSEL = 1, this field is 00h.

9.1.32 FLRCLV—FLR Capability Length and Value Register (SATA–D31:F5)

Address Offset: B2h–B3h
Attribute: RO, R/WO
Default Value: 2006h
Size: 16 bits
Function Level Reset: No (Bits 9:8 only)

When FLRCSSEL = 0, this register is RO:

Bit	Description
15:10	Reserved
9	**FLR Capability** — R/WO. This field indicates support for Function Level Reset.
8	**TXP Capability** — R/WO. This field indicates support for the Transactions Pending (TXP) bit. TXP must be supported if FLR is supported.
7:0	**Capability Length** — RO. This field indicates the number of bytes of the Vendor Specific capability as required by the PCI specification. It has the value of 06h for FLR Capability.

9.1.33 FLRCTRL—FLR Control Register (SATA–D31:F5)

Address Offset: B4h–B5h
Attribute: R/W, RO
Default Value: 0000h
Size: 16 bits

Bit	Description
15:9	Reserved
8	**Transactions Pending (TXP)** — RO. 0 = Completions for all Non-Posted requests have been received by the controller. 1 = Controller has issued Non-Posted request which has not been completed.
7:1	Reserved
0	**Initiate FLR** — R/W. Used to initiate FLR transition. A write of 1 indicates FLR transition.

9.1.34 ATC—APM Trapping Control Register (SATA–D31:F5)

Address Offset: C0h
Attribute: R/W
Default Value: 00h
Size: 8 bits

Note: This SATA controller does not support legacy I/O access. Therefore, this register is reserved. Software shall not change the default values of the register; otherwise, the result will be undefined.

Bit	Description
7:0	Reserved

9.1.35 ATC—APM Trapping Control Register (SATA–D31:F5)

Address Offset: C4h
Attribute: R/WC
Default Value: 00h
Size: 8 bits

Note: This SATA controller does not support legacy I/O access. Therefore, this register is reserved. Software shall not change the default values of the register; otherwise the result will be undefined.

Bit	Description
7:0	Reserved

9.2 Bus Master IDE I/O Registers (D31:F5)

The bus master IDE function uses 16 bytes of I/O space, allocated using the BAR register, located in D31:F2 Configuration space, offset 20h. All bus master IDE I/O space registers can be accessed as byte, word, or DWord quantities. Reading reserved bits returns an indeterminate, inconsistent value, and writes to reserved bits have no affect (but should not be attempted). These registers are only used for legacy operation. Software must not use these registers when running AHCI. The description of the I/O registers is shown in Table 9-2.

Table 9-2. Bus Master IDE I/O Register Address Map

BAR+ Offset	Mnemonic	Register	Default	Attribute
00	BMICP	Command Register Primary	00h	R/W
01	—	Reserved	—	RO
02	BMISP	Bus Master IDE Status Register Primary	00h	R/W, R/WC, RO
03	—	Reserved	—	RO
04–07	BMIDP	Bus Master IDE Descriptor Table Pointer Primary	xxxxxxxxh	R/W
08	BMICS	Command Register Secondary	00h	R/W
09	—	Reserved	—	RO
0Ah	BMISS	Bus Master IDE Status Register Secondary	00h	R/W, R/WC, RO
0Bh	—	Reserved	—	RO
0Ch–0Fh	BMIDS	Bus Master IDE Descriptor Table Pointer Secondary	xxxxxxxxh	R/W

9.2.1 BMIC[P,S]—Bus Master IDE Command Register (D31:F5)

Address Offset: Primary: BAR + 00h
Secondary: BAR + 08h
Attribute: R/W
Default Value: 00h
Size: 8 bits

Bit	Description
7:4	Reserved
3	**Read / Write Control (R/WC)** — R/W. This bit sets the direction of the bus master transfer: This bit must NOT be changed when the bus master function is active. 0 = Memory reads 1 = Memory writes
2:1	Reserved

Bit	Description
0	**Start/Stop Bus Master (START)** — R/W. 0 = All state information is lost when this bit is cleared. Master mode operation cannot be stopped and then resumed. If this bit is reset while bus master operation is still active (that is, the Bus Master IDE Active bit (D31:F5:BAR + 02h, bit 0) of the Bus Master IDE Status register for that IDE channel is set) and the drive has not yet finished its data transfer (the Interrupt bit in the Bus Master IDE Status register for that IDE channel is not set), the bus master command is said to be aborted and data transferred from the drive may be discarded instead of being written to system memory. 1 = Enables bus master operation of the controller. Bus master operation does not actually start unless the Bus Master Enable bit (D31:F5:04h, bit 2) in PCI configuration space is also set. Bus master operation begins when this bit is detected changing from 0 to 1. The controller will transfer data between the IDE device and memory only when this bit is set. Master operation can be halted by writing a 0 to this bit. ***Note:*** This bit is intended to be cleared by software after the data transfer is completed, as indicated by either the Bus Master IDE Active bit being cleared or the Interrupt bit of the Bus Master IDE Status register for that IDE channel being set, or both. Hardware does not clear this bit automatically. If this bit is cleared to 0 prior to the DMA data transfer being initiated by the drive in a device to memory data transfer, then Intel® Xeon® Processor D-1500 Product Family will not send DMAT to terminate the data transfer. SW intervention (such as, sending SRST) is required to reset the interface in this condition.

9.2.2 BMIS[P,S]—Bus Master IDE Status Register (D31:F5)

Address Offset:	Primary: BAR + 02h Secondary: BAR + 0Ah	Attribute:	R/W, R/WC, RO
Default Value:	00h	Size:	8 bits

Bit	Description
7	**PRD Interrupt Status (PRDIS)** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = This bit is set when the host controller execution of a PRD that has its PRD_INT bit set.
6	Reserved
5	**Drive 0 DMA Capable** — R/W. 0 = Not Capable 1 = Capable. Set by device dependent code (BIOS or device driver) to indicate that drive 0 for this channel is capable of DMA transfers, and that the controller has been initialized for optimum performance. Intel® Xeon® Processor D-1500 Product Family does not use this bit. It is intended for systems that do not attach BMIDE to the PCI bus.
4:3	Reserved
2	**Interrupt** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = Set when a device FIS is received with the 'I' bit set, provided that software has not disabled interrupts using the IEN bit of the Device Control Register (see chapter 5 of the *Serial ATA Specification*, Revision 1.0a).
1	**Error** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = This bit is set when the controller encounters a target abort or master abort when transferring data on PCI.
0	**Bus Master IDE Active (ACT)** — RO. 0 = This bit is cleared by Intel® Xeon® Processor D-1500 Product Family when the last transfer for a region is performed, where EOT for that region is set in the region descriptor. It is also cleared by Intel® Xeon® Processor D-1500 Product Family when the Start Bus Master bit (D31:F5:BAR+ 00h, bit 0) is cleared in the Command register. When this bit is read as a 0, all data transferred from the drive during the previous bus master command is visible in system memory, unless the bus master command was aborted. 1 = Set by Intel® Xeon® Processor D-1500 Product Family when the Start bit is written to the Command register.

9.2.3 BMID[P,S]—Bus Master IDE Descriptor Table Pointer Register (D31:F5)

Address Offset:	Primary: BAR + 04h–07h Secondary: BAR + 0Ch–0Fh	Attribute:	R/W
Default Value:	All bits undefined	Size:	32 bits

Bit	Description
31:2	**Address of Descriptor Table (ADDR)** — R/W. The bits in this field correspond to bits [31:2] of the memory location of the Physical Region Descriptor (PRD). The Descriptor Table must be DWord-aligned. The Descriptor Table must not cross a 64-K boundary in memory.
1:0	Reserved

9.3 Serial ATA Index/Data Pair Superset Registers

All of these I/O registers are in the core well. They are exposed only when SCC is 01h (that is, IDE programming interface) and the controller is not in combined mode. These are Index/Data Pair registers that are used to access the SerialATA superset registers (SerialATA Status, SerialATA Control and SerialATA Error). The I/O space for these registers is allocated through SIDPBA. Locations with offset from 08h to 0Fh are reserved for future expansion. Software-write operations to the reserved locations shall have no effect while software-read operations to the reserved locations shall return 0.

9.3.1 SINDX—SATA Index Register (D31:F5)

Address Offset:	SIDPBA + 00h	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits

Note: These are Index/Data Pair Registers that are used to access the SSTS, SCTL, and SERR. The I/O space for these registers is allocated through SIDPBA.

Bit	Description
31:16	Reserved
15:8	**Port Index (PIDX)**— R/W. This Index field is used to specify the port of the SATA controller at which the port-specific SSTS, SCTL, and SERR registers are located. 00h = Primary Master (Port 4) 02h = Secondary Master (Port 5) All other values are Reserved.
7:0	**Register Index (RIDX)**— R/W. This Index field is used to specify one out of three registers currently being indexed into. 00h = SSTS 01h = SCTL 02h = SERR All other values are Reserved.

9.3.2 SDATA—SATA Index Data Register (D31:F5)

Address Offset:	SIDPBA + 04h	Attribute:	R/W
Default Value:	All bits undefined	Size:	32 bits

Note: These are Index/Data Pair Registers that are used to access the SSTS, SCTL, and SERR. The I/O space for these registers is allocated through SIDPBA.

Bit	Description
31:0	**Data (DATA)**— R/W. This Data register is a "window" through which data is read or written to the memory mapped registers. A read or write to this Data register triggers a corresponding read or write to the memory mapped register pointed to by the Index register. The Index register must be setup prior to the read or write to this Data register. A physical register is not actually implemented as the data is actually stored in the memory mapped registers. Since this is not a physical register, the "default" value is the same as the default value of the register pointed to by Index.

9.3.2.1 PxSSTS—Serial ATA Status Register (D31:F5)

Address Offset:		Attribute:	RO
Default Value:	00000000h	Size:	32 bits

SDATA when SINDX.RIDX is 00h.

This is a 32-bit register that conveys the current state of the interface and host. Intel® Xeon® Processor D-1500 Product Family updates it continuously and asynchronously. When Intel® Xeon® Processor D-1500 Product Family transmits a COMRESET to the device, this register is updated to its reset values.

Bit	Description
31:12	Reserved
11:8	**Interface Power Management (IPM)** — RO**.** Indicates the current interface state: **Value** — **Description** 0h — Device not present or communication not established 1h — Interface in active state 2h — Interface in PARTIAL power management state 6h — Interface in SLUMBER power management state All other values reserved.
7:4	**Current Interface Speed (SPD)** — RO. Indicates the negotiated interface communication speed. **Value** — **Description** 0h — Device not present or communication not established 1h — Generation 1 communication rate negotiated 2h — Generation 2 communication rate negotiated 3h — Generation 3 communication rate negotiated All other values reserved. Intel® Xeon® Processor D-1500 Product Family Supports Gen 1 communication rates (1.5 Gb/s), Gen 2 rates (3.0 Gb/s) and Gen 3 rates (6.0 Gb/s).

Bit	Description
3:0	**Device Detection (DET)** — RO**.** Indicates the interface device detection and Phy state: **Value** — **Description** 0h — No device detected and Phy communication not established 1h — Device presence detected but Phy communication not established 3h — Device presence detected and Phy communication established 4h — Phy in offline mode as a result of the interface being disabled or running in a BIST loopback mode All other values reserved.

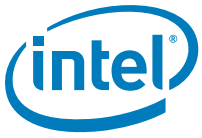
9.3.2.2 PxSCTL — Serial ATA Control Register (D31:F5)

Address Offset: Attribute: R/W, RO
Default Value: 00000004h Size: 32 bits

SDATA when SINDX.RIDX is 01h.

This is a 32-bit read-write register by which software controls SATA capabilities. Writes to the SControl register result in an action being taken by Intel® Xeon® Processor D-1500 Product Family or the interface. Reads from the register return the last value written to it.

Bit	Description
31:20	Reserved
19:16	Port Multiplier Port (PMP) — RO. This field is not used by AHCI.
15:12	Select Power Management (SPM) — RO. This field is not used by AHCI.
11:8	**Interface Power Management Transitions Allowed (IPM)** — R/W**.** Indicates which power states Intel® Xeon® Processor D-1500 Product Family is allowed to transition to: **Value** — **Description** 0h — No interface restrictions 1h — Transitions to the PARTIAL state disabled 2h — Transitions to the SLUMBER state disabled 3h — Transitions to both PARTIAL and SLUMBER states disabled All other values reserved
7:4	**Speed Allowed (SPD)** — R/W. Indicates the highest allowable speed of the interface. This speed is limited by the CAP.ISS (ABAR+00h:bit 23:20) field. **Value** — **Description** 0h — No speed negotiation restrictions 1h — Limit speed negotiation to Generation 1 communication rate 2h — Limit speed negotiation to Generation 2 communication rate 3h — Limit speed negotiation to Generation 3 communication rate All other values reserved. Intel® Xeon® Processor D-1500 Product Family Supports Gen 1 communication rates (1.5 Gb/s), Gen 2 rates (3.0 Gb/s) and Gen 3 rates (6 Gb/s).



Bit	Description
3:0	**Device Detection Initialization (DET)** — R/W**.** Controls Intel® Xeon® Processor D-1500 Product Famils device detection and interface initialization. **Value** — **Description** 0h — No device detection or initialization action requested 1h — Perform interface communication initialization sequence to establish communication. This is functionally equivalent to a hard reset and results in the interface being reset and communications re-initialized 4h — Disable the Serial ATA interface and put Phy in offline mode All other values reserved.

9.3.2.3 PxSERR—Serial ATA Error Register (D31:F5)

Address Offset: Attribute: R/WC
Default Value: 00000000h Size: 32 bits

SDATA when SINDx.RIDX is 02h.

Bits 26:16 of this register contains diagnostic error information for use by diagnostic software in validating correct operation or isolating failure modes. Bits 11:0 contain error information used by host software in determining the appropriate response to the error condition. If one or more of bits 11:8 of this register are set, the controller will stop the current transfer.

Bit	Description
31:27	Reserved
26	**Exchanged (X)** — R/WC. When set to 1, this bit indicates that a change in device presence has been detected since the last time this bit was cleared. This bit shall always be set to 1 anytime a COMINIT signal is received. This bit is reflected in the P0IS.PCS bit.
25	**Unrecognized FIS Type (F)** — R/WC. Indicates that one or more FISs were received by the Transport layer with good CRC, but had a type field that was not recognized.
24	**Transport state transition error (T)** — R/WC. Indicates that an error has occurred in the transition from one state to another within the Transport layer since the last time this bit was cleared.
23	**Link Sequence Error (S):** Indicates that one or more Link state machine error conditions was encountered. The Link Layer state machine defines the conditions under which the link layer detects an erroneous transition.
22	**Handshake (H)** — R/WC. Indicates that one or more R_ERR handshake response was received in response to frame transmission. Such errors may be the result of a CRC error detected by the recipient, a disparity or 8b/10b decoding error, or other error condition leading to a negative handshake on a transmitted frame.
21	**CRC Error (C)** — R/WC. Indicates that one or more CRC errors occurred with the Link Layer.
20	**Disparity Error (D)** — R/WC. This field is not used by AHCI.
19	**10b to 8b Decode Error (B)** — R/WC. Indicates that one or more 10b to 8b decoding errors occurred.
18	**Comm Wake (W)** — R/WC. Indicates that a Comm Wake signal was detected by the Phy.
17	**Phy Internal Error (I)** — R/WC. Indicates that the Phy detected some internal error.
16	**PhyRdy Change (N)** — R/WC. When set to 1, this bit indicates that the internal PhyRdy signal changed state since the last time this bit was cleared. In Intel® Xeon® Processor D-1500 Product Family, this bit will be set when PhyRdy changes from a 0 -> 1 or a 1 -> 0. The state of this bit is then reflected in the PxIS.PRCS interrupt status bit and an interrupt will be generated if enabled. Software clears this bit by writing a 1 to it.
15:12	Reserved
11	**Internal Error (E)** — R/WC. The SATA controller failed due to a master or target abort when attempting to access system memory.
10	**Protocol Error (P)** — R/WC. A violation of the Serial ATA protocol was detected. ***Note:*** Intel® Xeon® Processor D-1500 Product Family does not set this bit for all protocol violations that may occur on the SATA link.

Bit	Description
9	**Persistent Communication or Data Integrity Error (C)** — R/WC. A communication error that was not recovered occurred that is expected to be persistent. Persistent communications errors may arise from faulty interconnect with the device, from a device that has been removed or has failed, or a number of other causes.
8	**Transient Data Integrity Error (T)** — R/WC. A data integrity error occurred that was not recovered by the interface.
7:2	Reserved
1	**Recovered Communications Error (M)** — R/WC. Communications between the device and host was temporarily lost but was re-established. This can arise from a device temporarily being removed, from a temporary loss of Phy synchronization, or from other causes and may be derived from the PhyNRdy signal between the Phy and Link layers.
0	**Recovered Data Integrity Error (I)** — R/WC. A data integrity error occurred that was recovered by the interface through a retry operation or other recovery action.

§

10 EHCI Controller Registers (D29:F0)

10.1 USB EHCI Configuration Registers (USB EHCI—D29:F0)

Note: Prior to BIOS initialization of Intel® Xeon® Processor D-1500 Product Family USB subsystem, the EHCI controllers will appear as Function 7. After BIOS initialization, the EHCI controllers will be Function 0.

Note: Register address locations that are not shown in Table 10-1 should be treated as Reserved (see Section 4.2 for details).

Table 10-1. USB EHCI PCI Register Address Map (USB EHCI—D29:F0) (Sheet 1 of 2)

Offset	Mnemonic	Register Name	Default Value	Attribute
00h–01h	VID	Vendor Identification	8086h	RO
02h–03h	DID	Device Identification	See register description	RO
04h–05h	PCICMD	PCI Command	0000h	R/W, RO
06h–07h	PCISTS	PCI Status	0290h	R/W, RO
08h	RID	Revision Identification	See register description	RO
09h	PI	Programming Interface	20h	RO
0Ah	SCC	Sub Class Code	03h	RO
0Bh	BCC	Base Class Code	0Ch	RO
0Dh	PMLT	Primary Master Latency Timer	00h	RO
0Eh	HEADTYP	Header Type	00h	RO
10h–13h	MEM_BASE	Memory Base Address	00000000h	R/W, RO
2Ch–2Dh	SVID	USB EHCI Subsystem Vendor Identification	XXXXh	R/W
2Eh–2Fh	SID	USB EHCI Subsystem Identification	XXXXh	R/W
34h	CAP_PTR	Capabilities Pointer	50h	RO
3Ch	INT_LN	Interrupt Line	00h	R/W
3Dh	INT_PN	Interrupt Pin	See register description	RO
50h	PWR_CAPID	PCI Power Management Capability ID	01h	RO
51h	NXT_PTR1	Next Item Pointer	58h	R/W
52h–53h	PWR_CAP	Power Management Capabilities	C9C2h	R/W
54h–55h	PWR_CNTL_STS	Power Management Control / Status	0000h	R/W, R/WC, RO
58h	DEBUG_CAPID	Debug Port Capability ID	0Ah	RO
59h	NXT_PTR2	Next Item Pointer #2	98h	RWS
5Ah–5Bh	DEBUG_BASE	Debug Port Base Offset	20A0h	RO
60h	USB_RELNUM	USB Release Number	20h	RO
61h	FL_ADJ	Frame Length Adjustment	20h	R/W, RO
62h–63h	PWAKE_CAP	Port Wake Capabilities	07FFh	R/W, RO

Table 10-1. USB EHCI PCI Register Address Map (USB EHCI—D29:F0) (Sheet 2 of 2)

Offset	Mnemonic	Register Name	Default Value	Attribute
64h	PDO	Port Disable Override Register	0000h	R/W, RO
66h	RMHDEVR	RMH Device Removable Field Register	0000h	R/W, RO
68h–6Bh	LEG_EXT_CAP	USB EHCI Legacy Support Extended Capability	00000001h	R/W, RO
6Ch–6Fh	LEG_EXT_CS	USB EHCI Legacy Extended Support Control/Status	00000000h	R/W, R/WC, RO
70h–73h	SPECIAL_SMI	Intel Specific USB 2.0 SMI	00000000h	R/W, R/WC
74h–77h	OCMAP	Over-Current Mapping	C0300C03h	R/W
78h–7Dh	—	Reserved	—	—
7Eh–7Fh	RMHWKCTL	RMH Wake Control	0000h	R/W, RO
80h	ACCESS_CNTL	Access Control	00h	R/W, RO
84h–87h	EHCIIR1	EHCI Initialization Register 1	01h	R/W
98h	FLR_CID	FLR Capability ID	13h	RO
99h	FLR_NEXT	FLR Next Capability Pointer	00h	RO
9Ch	FLR_CTRL	FLR Control	00h	R/W, RO
9Dh	FLR_STS	FLR Status	00h	RO

Note: All configuration registers in this section are in the core well and reset by a core well reset and the D3-to-D0 warm reset, except as noted.

10.1.1 VID—Vendor Identification Register (USB EHCI—D29:F0)

Offset Address: 00h–01h Attribute: RO
Default Value: 8086h Size: 16 bits

Bit	Description
15:0	**Vendor ID** — RO. This is a 16-bit value assigned to Intel.

10.1.2 DID—Device Identification Register (USB EHCI—D29:F0)

Offset Address: 02h–03h Attribute: RO
Default Value: See bit description Size: 16 bits

Bit	Description
15:0	**Device ID** — RO. This is a 16-bit value assigned to Intel® Xeon® Processor D-1500 Product Family USB EHCI controller.

10.1.3 PCICMD—PCI Command Register (USB EHCI—D29:F0)

Address Offset: 04h–05h Attribute: R/W, RO
Default Value: 0000h Size: 16 bits

Bit	Description
15:11	Reserved Read Only
10	**Interrupt Disable** — R/W. 0 = The function is capable of generating interrupts. 1 = The function can not generate its interrupt to the interrupt controller. The corresponding Interrupt Status bit (D29:F0:06h, bit 3) is not affected by the interrupt enable.
9	Fast Back to Back Enable (FBE) — RO. Hardwired to 0.

Bit	Description
8	**SERR# Enable (SERR_EN)** — R/W. 0 = Disables EHC's capability to generate an SERR#. 1 = The Enhanced Host controller (EHC) is capable of generating (internally) SERR# in the following cases: • When it receive a completion status other than "successful" for one of its DMA initiated memory reads on it's internal interface. • When it detects an address or command parity error and the Parity Error Response bit is set. • When it detects a data parity error (when the data is going into the EHC) and the Parity Error Response bit is set.
7	Wait Cycle Control (WCC) — RO. Hardwired to 0.
6	**Parity Error Response (PER)** — R/W. 0 = The EHC is not checking for correct parity (on its internal interface). 1 = The EHC is checking for correct parity (on its internal interface) and halt operation when bad parity is detected during the data phase. ***Note:*** If the EHC detects bad parity on the address or command phases when the bit is set to 1, the host controller does not take the cycle. It halts the host controller (if currently not halted) and sets the Host System Error bit in the USBSTS register. This applies to both requests and completions from the system interface. This bit must be set in order for the parity errors to generate SERR#.
5	VGA Palette Snoop (VPS) — RO. Hardwired to 0.
4	Postable Memory Write Enable (PMWE) — RO. Hardwired to 0.
3	Special Cycle Enable (SCE) — RO. Hardwired to 0.
2	**Bus Master Enable (BME)** — R/W. 0 = Disables this functionality. 1 = Enables Intel® Xeon® Processor D-1500 Product Family to act as a master on the PCI bus for USB transfers.
1	**Memory Space Enable (MSE)** — R/W. This bit controls access to the USB 2.0 Memory Space registers. 0 = Disables this functionality. 1 = Enables accesses to the USB 2.0 registers. The Base Address register (D29:F0:10h) for USB 2.0 should be programmed before this bit is set.
0	I/O Space Enable (IOSE) — RO. Hardwired to 0.

10.1.4 PCISTS—PCI Status Register (USB EHCI—D29:F0)

Address Offset:	06h–07h	Attribute:	R/WC, RO
Default Value:	0290h	Size:	16 bits

Note: For the writable bits, software must write a 1 to clear bits that are set. Writing a 0 to the bit has no effect.

Bit	Description
15	**Detected Parity Error (DPE)** — R/WC. 0 = No parity error detected. 1 = This bit is set by Intel® Xeon® Processor D-1500 Product Family when a parity error is seen by the EHCI controller, regardless of the setting of bit 6 or bit 8 in the Command register or any other conditions.
14	**Signaled System Error (SSE)** — R/WC. 0 = No SERR# signaled by Intel® Xeon® Processor D-1500 Product Family. 1 = This bit is set by Intel® Xeon® Processor D-1500 Product Family when it signals SERR# (internally). The SER_EN bit (bit 8 of the Command Register) must be 1 for this bit to be set.
13	**Received Master Abort (RMA)** — R/WC. 0 = No master abort received by EHC on a memory access. 1 = This bit is set when EHC, as a master, receives a master abort status on a memory access. This is treated as a Host Error and halts the DMA engines. This event can optionally generate an SERR# by setting the SERR# Enable bit.

Bit	Description
12	**Received Target Abort (RTA)** — R/WC. 0 = No target abort received by EHC on memory access. 1 = This bit is set when EHC, as a master, receives a target abort status on a memory access. This is treated as a Host Error and halts the DMA engines. This event can optionally generate an SERR# by setting the SERR# Enable bit (D29:F0:04h, bit 8).
11	Signaled Target Abort (STA) — RO. This bit is used to indicate when the EHCI function responds to a cycle with a target abort. There is no reason for this to happen, so this bit is hardwired to 0.
10:9	DEVSEL# Timing Status (DEVT_STS) — RO. This 2-bit field defines the timing for DEVSEL# assertion. Read Only
8	**Master Data Parity Error Detected (DPED)** — R/WC. 0 = No data parity error detected on USB2.0 read completion packet. 1 = This bit is set by Intel® Xeon® Processor D-1500 Product Family when a data parity error is detected on a USB 2.0 read completion packet on the internal interface to the EHCI host controller and bit 6 of the Command register is set to 1.
7	Fast Back to Back Capable (FB2BC) — RO. Hardwired to 1.
6	User Definable Features (UDF) — RO. Hardwired to 0.
5	66 MHz Capable (66 MHz _CAP) — RO. Hardwired to 0.
4	Capabilities List (CAP_LIST) — RO. Hardwired to 1 indicating that offset 34h contains a valid capabilities pointer.
3	**Interrupt Status** — RO. This bit reflects the state of this function's interrupt at the input of the enable/disable logic. 0 = This bit will be 0 when the interrupt is de-asserted. 1 = This bit is a 1 when the interrupt is asserted. The value reported in this bit is independent of the value in the Interrupt Enable bit.
2:0	Reserved

10.1.5 RID—Revision Identification Register (USB EHCI—D29:F0)

Offset Address: 08h — Attribute: RO
Default Value: See bit description — Size: 8 bits

Bit	Description
7:0	**Revision ID** — RO. This field indicates the device specific revision identifier.

10.1.6 PI—Programming Interface Register (USB EHCI—D29:F0)

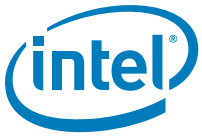
Address Offset: 09h — Attribute: RO
Default Value: 20h — Size: 8 bits

Bit	Description
7:0	**Programming Interface** — RO. A value of 20h indicates that this USB 2.0 host controller conforms to the EHCI Specification.

10.1.7 SCC—Sub Class Code Register (USB EHCI—D29:F0)

Address Offset: 0Ah — Attribute: RO
Default Value: 03h — Size: 8 bits

Bit	Description
7:0	**Sub Class Code (SCC)** — RO. 03h = Universal serial bus host controller.



10.1.8 BCC—Base Class Code Register (USB EHCI—D29:F0)

Address Offset: 0Bh
Default Value: 0Ch
Attribute: RO
Size: 8 bits

Bit	Description
7:0	**Base Class Code (BCC)** — RO. 0Ch = Serial bus controller.

10.1.9 PMLT—Primary Master Latency Timer Register (USB EHCI—D29:F0)

Address Offset: 0Dh
Default Value: 00h
Attribute: RO
Size: 8 bits

Bit	Description
7:0	**Master Latency Timer Count (MLTC)** — RO. Hardwired to 00h. Because the EHCI controller is internally implemented with arbitration on an interface (and not PCI), it does not need a master latency timer.

10.1.10 HEADTYP—Header Type Register (USB EHCI—D29:F0)

Address Offset: 0Eh
Default Value: 00h
Attribute: RO
Size: 8 bits

Bit	Description
7	**Multi-Function Device** — RO. When set to '1' indicates this is a multifunction device: 0 = Single-function device 1 = Multi-function device.
6:0	Configuration Layout. Hardwired to 00h, which indicates the standard PCI configuration layout.

10.1.11 MEM_BASE—Memory Base Address Register (USB EHCI—D29:F0)

Address Offset: 10h–13h
Default Value: 00000000h
Attribute: R/W, RO
Size: 32 bits

Bit	Description
31:10	**Base Address** — R/W. Bits [31:10] correspond to memory address signals [31:10], respectively. This gives 1-KB of locatable memory space aligned to 1-KB boundaries.
9:4	Reserved
3	**Prefetchable** — RO. Hardwired to 0 indicating that this range should not be prefetched.
2:1	**Type** — RO. Hardwired to 00b indicating that this range can be mapped anywhere within 32-bit address space.
0	**Resource Type Indicator (RTE)** — RO. Hardwired to 0 indicating that the base address field in this register maps to memory space.

10.1.12 SVID—USB EHCI Subsystem Vendor ID Register (USB EHCI—D29:F0)

Address Offset:	2Ch–2Dh	Attribute:	R/W
Default Value:	XXXXh	Size:	16 bits
Reset:	None	Power Well:	Core

Bit	Description
15:0	**Subsystem Vendor ID (SVID)** — R/W. This register, in combination with the USB 2.0 Subsystem ID register, enables the operating system to distinguish each subsystem from the others. ***Note:*** Writes to this register are enabled when the WRT_RDONLY bit (D29:F0:80h, bit 0) is set to 1.

10.1.13 SID—USB EHCI Subsystem ID Register (USB EHCI—D29:F0)

Address Offset:	2Eh–2Fh	Attribute:	R/W
Default Value:	XXXXh	Size:	16 bits
Reset:	None	Power Well:	Core

Bit	Description
15:0	**Subsystem ID (SID)** — R/W. BIOS sets the value in this register to identify the Subsystem ID. This register, in combination with the Subsystem Vendor ID register, enables the operating system to distinguish each subsystem from other(s). ***Note:*** Writes to this register are enabled when the WRT_RDONLY bit (D29:F0:80h, bit 0) is set to 1.

10.1.14 CAP_PTR—Capabilities Pointer Register (USB EHCI—D29:F0)

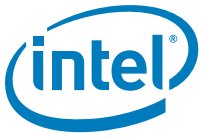
Address Offset:	34h	Attribute:	RO
Default Value:	50h	Size:	8 bits
Power Well:	Core		

Bit	Description
7:0	**Capabilities Pointer (CAP_PTR)** — RO. This register points to the starting offset of the USB 2.0 capabilities ranges.

10.1.15 INT_LN—Interrupt Line Register (USB EHCI—D29:F0)

Address Offset:	3Ch	Attribute:	R/W
Default Value:	00h	Size:	8 bits
Reset:	No	Power Well:	Core

Bit	Description
7:0	**Interrupt Line (INT_LN)** — R/W. This data is not used by Intel® Xeon® Processor D-1500 Product Family. It is used as a scratchpad register to communicate to software the interrupt line that the interrupt pin is connected to.



10.1.16 INT_PN—Interrupt Pin Register (USB EHCI—D29:F0)

Address Offset: 3Dh Attribute: RO
Default Value: See Description Size: 8 bits

Bit	Description
7:0	**Interrupt Pin** — RO. This reflects the value of D29IP.E1IP (Chipset Config Registers:Offset 3108:bits 3:0) or D26IP.E2IP (Chipset Config Registers:Offset 3114:bits 3:0). ***Note:*** As a single function device, only INTA# may be used while the other three interrupt lines have no meaning. (refer to PCI 3.0 specification, Section 2.2.6, Interrupt Pins). ***Note:*** Bits 7:4 are always 0h

10.1.17 PWR_CAPID—PCI Power Management Capability Identification Register (USB EHCI—D29:F0)

Address Offset: 50h Attribute: RO
Default Value: 01h Size: 8 bits

Bit	Description
7:0	**Power Management Capability ID** — RO. A value of 01h indicates that this is a PCI Power Management capabilities field.

10.1.18 NXT_PTR1—Next Item Pointer #1 Register (USB EHCI—D29:F0)

Address Offset: 51h Attribute: R/W
Default Value: 58h Size: 8 bits
Power Well: Core

Bit	Description
7:0	**Next Item Pointer 1 Value** — R/W (special). This register defaults to 58h that indicates that the next capability registers begin at configuration offset 58h. This register is writable when the WRT_RDONLY bit (D29:F0:80h, bit 0) is set. This allows BIOS to effectively hide the Debug Port capability registers, if necessary. This register should only be written during system initialization before the plug-and-play software has enabled any master-initiated traffic. Only values of 58h (Debug Port and FLR capabilities visible) and 98h (Debug Port invisible, next capability is FLR) are expected to be programmed in this register. ***Note:*** Register not reset by D3-to-D0 warm reset.

10.1.19 PWR_CAP—Power Management Capabilities Register (USB EHCI—D29:F0)

Address Offset: 52h–53h Attribute: R/W, RO
Default Value: C9C2h Size: 16 bits
Power Well: Core

Bit	Description
15:11	**PME Support (PME_SUP)** — R/W. This 5-bit field indicates the power states in which the function may assert PME#. Intel® Xeon® Processor D-1500 Product Family EHC does not support the D1 or D2 states. For all other states, Intel® Xeon® Processor D-1500 Product Family EHC is capable of generating PME#. Software should never need to modify this field.
10	D2 Support (D2_SUP) — RO. 0 = D2 State is not supported
9	D1 Support (D1_SUP) — RO. 0 = D1 State is not supported
8:6	**Auxiliary Current (AUX_CUR)** — R/W**.** Intel® Xeon® Processor D-1500 Product Family EHC reports 375 mA maximum suspend well current required when in the $D3_{COLD}$ state.

Bit	Description
5	**Device Specific Initialization (DSI)**— RO. Intel® Xeon® Processor D-1500 Product Family reports 0, indicating that no device-specific initialization is required.
4	Reserved
3	**PME Clock (PME_CLK)** — RO. Intel® Xeon® Processor D-1500 Product Family reports 0, indicating that no PCI clock is required to generate PME#.
2:0	**Version (VER)** — RO. Intel® Xeon® Processor D-1500 Product Family reports 010b, indicating that it complies with Revision 1.1 of the PCI Power Management Specification.

Notes:
1. Normally, this register is read-only to report capabilities to the power management software. To report different power management capabilities, depending on the system in which Intel® Xeon® Processor D-1500 Product Family is used, bits 15:11 and 8:6 in this register are writable when the WRT_RDONLY bit (D29:F0:80h, bit 0) is set. The value written to this register does not affect the hardware other than changing the value returned during a read.
2. Reset: core well, but not D3-to-D0 warm reset.

10.1.20 PWR_CNTL_STS—Power Management Control / Status Register (USB EHCI—D29:F0)

Address Offset: 54h–55h
Attribute: R/W, R/WC, RO
Default Value: 0000h
Size: 16 bits
Power Well Bits 1,0:Core; Power Well Bits 15,8: Suspend

Bit	Description
15	**PME Status** — R/WC. 0 = Writing a 1 to this bit will clear it and cause the internal PME to de-assert (if enabled). 1 = This bit is set when Intel® Xeon® Processor D-1500 Product Family EHC would normally assert the PME# signal independent of the state of the PME_En bit. ***Note:*** This bit must be explicitly cleared by the operating system each time the operating system is loaded. This bit is not reset by Function Level Reset.
14:13	Data Scale — RO. Hardwired to 00b indicating it does not support the associated Data register.
12:9	Data Select — RO. Hardwired to 0000b indicating it does not support the associated Data register.
8	**PME Enable** — R/W. 0 = Disable. 1 = Enables Intel® Xeon® Processor D-1500 Product Family EHC to generate an internal PME signal when PME_Status is 1. ***Note:*** This bit must be explicitly cleared by the operating system each time it is initially loaded. This bit is not reset by Function Level Reset.
7:2	Reserved
1:0	**Power State** — R/W. This 2-bit field is used both to determine the current power state of EHC function and to set a new power state. The definition of the field values are: 00 = D0 state 11 = $D3_{HOT}$ state If software attempts to write a value of 10b or 01b in to this field, the write operation must complete normally; however, the data is discarded and no state change occurs. When in the $D3_{HOT}$ state, Intel® Xeon® Processor D-1500 Product Family must not accept accesses to the EHC memory range; but the configuration space must still be accessible. When not in the D0 state, the generation of the interrupt output is blocked. Specifically, the PIRQH is not asserted by Intel® Xeon® Processor D-1500 Product Family when not in the D0 state. When software changes this value from the $D3_{HOT}$ state to the D0 state, an internal warm (soft) reset is generated, and software must re-initialize the function.

Note: Reset (bits 15, 8): suspend well, and not D3-to-D0 warm reset nor core well reset.

10.1.21 DEBUG_CAPID—Debug Port Capability ID Register (USB EHCI—D29:F0)

Address Offset: 58h
Default Value: 0Ah
Attribute: RO
Size: 8 bits

Bit	Description
7:0	**Debug Port Capability ID** — RO. Hardwired to 0Ah indicating that this is the start of a Debug Port Capability structure.

10.1.22 NXT_PTR2—Next Item Pointer #2 Register (USB EHCI—D29:F0)

Address Offset: 59h
Default Value: 98h
Attribute: RO
Size: 8 bits
Function Level Reset: No

Bit	Description
7:0	**Next Item Pointer 2 Capability** — RO. This register points to the next capability in the Function Level Reset capability structure.

10.1.23 DEBUG_BASE—Debug Port Base Offset Register (USB EHCI—D29:F0)

Address Offset: 5Ah–5Bh
Default Value: 20A0h
Attribute: RO
Size: 16 bits

Bit	Description
15:13	**BAR Number** — RO. Hardwired to 001b to indicate the memory BAR begins at offset 10h in the EHCI configuration space.
12:0	**Debug Port Offset** — RO. Hardwired to 0A0h to indicate that the Debug Port registers begin at offset A0h in the EHCI memory range.

10.1.24 USB_RELNUM—USB Release Number Register (USB EHCI—D29:F0)

Address Offset: 60h
Default Value: 20h
Attribute: RO
Size: 8 bits

Bit	Description
7:0	**USB Release Number** — RO. A value of 20h indicates that this controller follows *Universal Serial Bus (USB) Specification, Revision 2.0*.

10.1.25 FL_ADJ—Frame Length Adjustment Register (USB EHCI—D29:F0)

Address Offset: 61h
Default Value: 20h
Attribute: R/W
Size: 8 bits
Function Level Reset: No
Power Well: Suspend

This feature is used to adjust any offset from the clock source that generates the clock that drives the SOF counter. When a new value is written into these six bits, the length of the frame is adjusted. Its initial programmed value is system dependent based on the accuracy of hardware USB clock and is initialized by system BIOS. This register should only be modified when the HChalted bit (D29:F0:CAPLENGTH + 24h, bit 12) in the USB2.0_STS register is a 1. Changing value of this register while the host controller

is operating yields undefined results. It should not be reprogrammed by USB system software unless the default or BIOS programmed values are incorrect, or the system is restoring the register while returning from a suspended state.

These bits in suspend well and not reset by a D3-to-D0 warm rest or a core well reset.

Bit	Description
7:6	Reserved — RO. These bits are reserved for future use and should read as 00b.
5:0	**Frame Length Timing Value** — R/W. Each decimal value change to this register corresponds to 16 high-speed bit times. The SOF cycle time (number of SOF counter clock periods to generate a SOF micro-frame length) is equal to 59488 + value in this field. The default value is decimal 32 (20h) that gives a SOF cycle time of 60000. Frame Length (# 480 MHz Clocks) (decimal) — Frame Length Timing Value (this register) (decimal) 59488 — 0 59504 — 1 59520 — 2 — — — 59984 — 31 60000 — 32 — — — 60480 — 62 60496 — 63

10.1.26 PWAKE_CAP—Port Wake Capability Register (USB EHCI—D29:F0)

Address Offset: 62–63h
Default Value: 07FFh
Function Level Reset: No
Attribute: R/W, RO
Size: 16 bits
Power Well: Suspend

This register is in the suspend power well. The intended use of this register is to establish a policy about which ports are to be used for wake events. Bit positions 1-8(D29)in the mask correspond to a physical port implemented on the current EHCI controller. A 1 in a bit position indicates that a device connected below the port can be enabled as a wake-up device and the port may be enabled for disconnect/connect or overcurrent events as wake-up events. This is an information-only mask register. The bits in this register **do not** affect the actual operation of the EHCI host controller. The system-specific policy can be established by BIOS initializing this register to a system-specific value. System software uses the information in this register when enabling devices and ports for remote wake-up.

These bits are not reset by a D3-to-D0 warm rest or a core well reset.

Bit	Description
15:11	Reserved, Read Only
10:1 (D29)	**Port Wake Up Capability Mask** — R/W. Bit positions 1-10 correspond to a physical port implemented on this host controller. For example, bit position 1 corresponds to port 1, bit position 2 corresponds to port 2, and so on.
0	**Port Wake Implemented** — R/W. A 1 in this bit indicates that this register is implemented to software.

10.1.27 PDO—Port Disable Override Register

Address Offset: 64h
Default Value: 0000h
Power Well: Suspend
Attribute: R/W, RO
Size: 16 bits

Bit	Description
15:8	Reserved, Read Only
7:0	USB Port Disable: A '1' in a bit position prevents the corresponding USB port from reporting a Device Connection to the hub. Attempts to enable the port will be ignored by the hardware when this bit is 1. This register cannot be written when the USB Per-Port Registers Write Enable bit (in Power Management I/O Space) is 0.

10.1.28 RMHDEVR—RMH Device Removable Field Register

Address Offset: 66h
Default Value: 0000h
Power Well: Suspend
Attribute: R/W, RO
Size: 16 bits

Bit	Description
15:9	Reserved, Read Only
8:1	Device Removable Bit Map: A '1' in a given bit position in this field indicates that the corresponding downstream port of the RMH is connected to a non-removable device. A '0' indicates that the port is exposed to the user. Bits 8:1 are mapped to Ports 8:1 (on EHCI #1, Device. 29) This bits control the value returned by the RMH in the Deviceremovable field of the Hub Descriptor. A '1' in a given bit position in this register will result in the corresponding bit in the DeviceRemovable field of the hub descriptor being set to '1' as well (indicating that the port is connected to a non-removable device). System BIOS is expected to set these values upon Boot and resume from Sx states. ***Note:*** Bits 8:5 are reserved (maintained as RW but with no significance) for since RMH corresponding to EHCI has only 4 ports.
0	Reserved, Read Only

10.1.29 LEG_EXT_CAP—USB EHCI Legacy Support Extended Capability Register (USB EHCI—D29:F0)

Address Offset: 68–6Bh
Default Value: 00000001h
Power Well: Suspend
Function Level Reset: No
Attribute: R/W, RO
Size: 32 bits

Note: These bits are not reset by a D3-to-D0 warm rest or a core well reset.

Bit	Description
31:25	Reserved — RO. Hardwired to 00h
24	**HC OS Owned Semaphore** — R/W. System software sets this bit to request ownership of the EHCI controller. Ownership is obtained when this bit reads as 1 and the HC BIOS Owned Semaphore bit reads as clear.
23:17	Reserved — RO. Hardwired to 00h
16	**HC BIOS Owned Semaphore** — R/W. The BIOS sets this bit to establish ownership of the EHCI controller. System BIOS will clear this bit in response to a request for ownership of the EHCI controller by system software.
15:8	**Next EHCI Capability Pointer** — RO. Hardwired to 00h to indicate that there are no EHCI Extended Capability structures in this device.
7:0	**Capability ID** — RO. Hardwired to 01h to indicate that this EHCI Extended Capability is the Legacy Support Capability.

10.1.30 LEG_EXT_CS—USB EHCI Legacy Support Extended Control / Status Register (USB EHCI—D29:F0)

Address Offset: 6C–6Fh
Attribute: R/W, R/WC, RO
Default Value: 00000000h
Size: 32 bits
Power Well: Suspend
Function Level Reset: No

Note: These bits are not reset by a D3-to-D0 warm rest or a core well reset.

Bit	Description
31	**SMI on BAR** — R/WC. Software clears this bit by writing a 1 to it. 0 = Base Address Register (BAR) not written. 1 = This bit is set to 1 when the Base Address Register (BAR) is written.
30	**SMI on PCI Command** — R/WC. Software clears this bit by writing a 1 to it. 0 = PCI Command (PCICMD) Register Not written. 1 = This bit is set to 1 when the PCI Command (PCICMD) Register is written.
29	**SMI on OS Ownership Change** — R/WC. Software clears this bit by writing a 1 to it. 0 = No HC OS Owned Semaphore bit change. 1 = This bit is set to 1 when the HC OS Owned Semaphore bit in the LEG_EXT_CAP register (D29:F0:68h, bit 24) transitions from 1 to 0 or 0 to 1.
28:22	Reserved
21	**SMI on Async Advance** — RO. This bit is a shadow bit of the Interrupt on Async Advance bit (D29:F0:CAPLENGTH + 24h, bit 5) in the USB2.0_STS register. ***Note:*** To clear this bit system software must write a 1 to the Interrupt on Async Advance bit in the USB2.0_STS register.
20	**SMI on Host System Error** — RO. This bit is a shadow bit of Host System Error bit in the USB2.0_STS register (D29:F0:CAPLENGTH + 24h, bit 4). ***Note:*** To clear this bit system software must write a 1 to the Host System Error bit in the USB2.0_STS register.
19	**SMI on Frame List Rollover** — RO. This bit is a shadow bit of Frame List Rollover bit (D29:F0:CAPLENGTH + 24h, bit 3) in the USB2.0_STS register. ***Note:*** To clear this bit system software must write a 1 to the Frame List Rollover bit in the USB2.0_STS register.
18	**SMI on Port Change Detect** — RO. This bit is a shadow bit of Port Change Detect bit (D29:F0:CAPLENGTH + 24h, bit 2) in the USB2.0_STS register. ***Note:*** To clear this bit system software must write a 1 to the Port Change Detect bit in the USB2.0_STS register.
17	**SMI on USB Error** — RO. This bit is a shadow bit of USB Error Interrupt (USBERRINT) bit (D29:F0:CAPLENGTH + 24h, bit 1) in the USB2.0_STS register. ***Note:*** To clear this bit system software must write a 1 to the USB Error Interrupt bit in the USB2.0_STS register.
16	**SMI on USB Complete** — RO. This bit is a shadow bit of USB Interrupt (USBINT) bit (D29:F0:CAPLENGTH + 24h, bit 0) in the USB2.0_STS register. ***Note:*** To clear this bit system software must write a 1 to the USB Interrupt bit in the USB2.0_STS register.
15	**SMI on BAR Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is 1 and SMI on BAR (D29:F0:6Ch, bit 31) is 1, then the host controller will issue an SMI.
14	**SMI on PCI Command Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is 1 and SMI on PCI Command (D29:F0:6Ch, bit 30) is 1, then the host controller will issue an SMI.
13	**SMI on OS Ownership Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1 AND the OS Ownership Change bit (D29:F0:6Ch, bit 29) is 1, the host controller will issue an SMI.
12:6	Reserved

Bit	Description
5	**SMI on Async Advance Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1, and the SMI on Async Advance bit (D29:F0:6Ch, bit 21) is a 1, the host controller will issue an SMI immediately.
4	**SMI on Host System Error Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1, and the SMI on Host System Error (D29:F0:6Ch, bit 20) is a 1, the host controller will issue an SMI.
3	**SMI on Frame List Rollover Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1, and the SMI on Frame List Rollover bit (D29:F0:6Ch, bit 19) is a 1, the host controller will issue an SMI.
2	**SMI on Port Change Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1, and the SMI on Port Change Detect bit (D29:F0:6Ch, bit 18) is a 1, the host controller will issue an SMI.
1	**SMI on USB Error Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1, and the SMI on USB Error bit (D29:F0:6Ch, bit 17) is a 1, the host controller will issue an SMI immediately.
0	**SMI on USB Complete Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1, and the SMI on USB Complete bit (D29:F0:6Ch, bit 16) is a 1, the host controller will issue an SMI immediately.

10.1.31 SPECIAL_SMI—Intel® Specific USB 2.0 SMI Register (USB EHCI—D29:F0)

Address Offset: 70h–73h
Attribute: R/W, R/WC
Default Value: 00000000h
Size: 32 bits
Power Well: Suspend
Function Level Reset: No

Note: These bits are not reset by a D3-to-D0 warm rest or a core well reset.

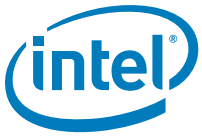
Bit	Description
31:25	Reserved
24:22	**SMI on PortOwner** — R/WC. Software clears these bits by writing a 1 to it. 0 = No Port Owner bit change. 1 = Bits 24:22 correspond to the Port Owner bits for ports 0 (22) through 3 (24). These bits are set to 1 when the associated Port Owner bits transition from 0 to 1 or 1 to 0.
21	**SMI on PMCSR** — R/WC. Software clears these bits by writing a 1 to it. 0 = Power State bits Not modified. 1 = Software modified the Power State bits in the Power Management Control/Status (PMCSR) register (D29:F0:54h).
20	**SMI on Async** — R/WC. Software clears these bits by writing a 1 to it. 0 = No Async Schedule Enable bit change 1 = Async Schedule Enable bit transitioned from 1 to 0 or 0 to 1.
19	**SMI on Periodic** — R/WC. Software clears this bit by writing a 1 it. 0 = No Periodic Schedule Enable bit change. 1 = Periodic Schedule Enable bit transitions from 1 to 0 or 0 to 1.
18	**SMI on CF** — R/WC. Software clears this bit by writing a 1 it. 0 = No Configure Flag (CF) change. 1 = Configure Flag (CF) transitions from 1 to 0 or 0 to 1.
17	**SMI on HCHalted** — R/WC. Software clears this bit by writing a 1 it. 0 = HCHalted did Not transition to 1 (as a result of the Run/Stop bit being cleared). 1 = HCHalted transitions to 1 (as a result of the Run/Stop bit being cleared).

Bit	Description
16	**SMI on HCReset** — R/WC. Software clears this bit by writing a 1 it. 0 = HCRESET did Not transitioned to 1. 1 = HCRESET transitioned to 1.
15:6	**SMI on PortOwner Enable** — R/W. 0 = Disable. 1 = Enable. When any of these bits are 1 and the corresponding SMI on PortOwner bits are 1, then the host controller will issue an SMI. Unused ports should have their corresponding bits cleared.
5	**SMI on PMSCR Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is 1 and SMI on PMSCR is 1, then the host controller will issue an SMI.
4	**SMI on Async Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is 1 and SMI on Async is 1, then the host controller will issue an SMI
3	**SMI on Periodic Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is 1 and SMI on Periodic is 1, then the host controller will issue an SMI.
2	**SMI on CF Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is 1 and SMI on CF is 1, then the host controller will issue an SMI.
1	**SMI on HCHalted Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1 and SMI on HCHalted is 1, then the host controller will issue an SMI.
0	**SMI on HCReset Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1 and SMI on HCReset is 1, then host controller will issue an SMI.

10.1.32 OCMAP—Over-Current Mapping Register

Address Offset: 74-77h
Default Value: C0300C03h
Function Level Reset: No
Attribute: R/W
Size: 32 bits
Power well: Suspend

Bit	Description
31:24	OC3 Mapping Each bit position maps OC3 (EHCI 1) to a set of ports as follows: EHCI 1: Map OC3 **Bit: 31 30 29 28 27 26 25 24** **Port: X X X X 3 2 1 0** It is software responsibility to ensure that a given port's bit map is set only for one OC pin.
23:16	OC2 Mapping Each bit position maps OC2 (EHCI 1) to a set of ports as follows: EHCI 1: Map OC2 **Bit: 23 22 21 20 19 18 17 16** **Port: X X X X 3 2 1 0** It is software responsibility to ensure that a given port's bit map is set only for one OC pin.



Bit	Description
15:08	OC1Mapping Each bit position maps OC1 (EHCI 1) to a set of ports as follows: EHCI 1: Map OC1 **Bit: 15 14 13 12 11 10 9 8** **Port: X X X X 3 2 1 0** It is software responsibility to ensure that a given port's bit map is set only for one OC pin.
07:00	OC0 Mapping Each bit position maps OC0 (EHCI 1) to a set of ports as follows: EHCI 1: Map OC0 **Bit: 7 6 5 4 3 2 1 0** **Port: X X X X 3 2 1 0** It is software responsibility to ensure that a given port's bit map is set only for one OC pin.

10.1.33 RMHWKCTL—RMH Wake Control Register

Address Offset: 7Eh
Default Value: 0000h
Function Level Reset: No
Attribute: R/W, RO
Size: 16 bits
Power well: Suspend

Bit	Description
15:09	Reserved
08	**RMH Inherit EHCI Wake Control Settings** -R/W: 0 = bits 2:0 of this register **DO NOT** reflect the appropriate bits of EHCI PORTSC0 bits 22:20. 1 = Bits 2:0 of this register reflect the appropriate bits of EHCI PORTSC0 bits 22:20.
07:04	Reserved
03	**RMH Upstream Wake on Device Resume Disable**- R/W 0 = The RMH will initiate a resume on its upstream port and cause a wake when a device resume occurs on an enabled downstream port 1 = The RMH will **NOT** initiate a resume on its upstream port and cause a wake when a device resume occurs on an enabled downstream port
02	**RMH Upstream Wake on OC Disable** - R/W 0 = The RMH will initiate a resume on its upstream port and cause a wake when over-current condition occurs downstream port 1 = The RMH will **NOT** initiate a resume on its upstream port and cause a wake when over-current condition occurs downstream port
01	**RMH Upstream Wake on Disconnect Disable -** R/W 0 = The RMH will initiate a resume on its upstream port and cause a wake when a disconnect event occurs on a downstream port 1 = The RMH will **NOT** initiate a resume on its upstream port and cause a wake when a disconnect event occurs on a downstream port
00	**RMH Upstream Wake on Connect Disable**- R/W 0 = The RMH will initiate a resume on its upstream port and cause a wake when a connect event occurs on a downstream port 1 = The RMH will **NOT** initiate a resume on its upstream port and cause a wake when a connect event occurs on a downstream port

10.1.34 ACCESS_CNTL—Access Control Register (USB EHCI—D29:F0)

Address Offset: 80h
Default Value: 00h
Attribute: R/W
Size: 8 bits
Function Level Reset: No

Bit	Description
7:1	Reserved
0	**WRT_RDONLY** — R/W. When set to 1, this bit enables a select group of normally read-only registers in the EHC function to be written by software. Registers that may only be written when this mode is entered are noted in the summary tables and detailed description as "Read/Write-Special". The registers fall into two categories: 1. System-configured parameters 2. Status bits

10.1.35 EHCIIR1—EHCI Initialization Register 1 (USB EHCI—D29:F0)

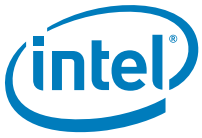
Address Offset: 84h
Default Value: 01h
Attribute: R/W
Size: 32 bits
Power well: Core

Bit	Description
31:29	Reserved
28	**EHCI Prefetch Entry Clear** — R/W. 0 = EHC will clear prefetched entries in DMA. 1 = EHC will not clear prefetched entries in DMA
27:5	Reserved
4	**Intel® Pre-fetch Based Pause Enable** — R/W. 0 = Intel Pre-fetch Based Pause is disabled. 1 = Intel Pre-fetch Based Pause is enabled.
3:0	Reserved

10.1.36 FLR_CID—Function Level Reset Capability ID Register (USB EHCI—D29:F0)

Address Offset: 98h
Default Value: 13h
Attribute: RO
Size: 8 bits
Function Level Reset: No

Bit	Description
7:0	**Capability ID** — RO. 13h = Capability ID



10.1.37 FLR_NEXT—Function Level Reset Next Capability Pointer Register (USB EHCI—D29:F0)

Address Offset: 99h
Default Value: 00h
Attribute: RO
Size: 8 bits
Function Level Reset: No

Bit	Description
7:0	A value of 00h in this register indicates this is the last capability field.

10.1.38 FLR_CLV—Function Level Reset Capability Length and Version Register (USB EHCI—D29:F0)

Address Offset: 9Ah–9Bh
Default Value: 0306h
Attribute: R/WO, RO
Size: 16 bits
Function Level Reset: No

When FLRCSSEL = 0, this register is defined as follows:

Bit	Description
15:10	Reserved
9	**FLR Capability** — R/WO. 1 = Support for Function Level Reset (FLR).
8	**TXP Capability** — R/WO. 1 = Support for Transactions Pending (TXP) bit. TXP must be supported if FLR is supported.
7:0	**Capability Length** — RO. This field indicates the # of bytes of this vendor specific capability as required by the PCI specification. It has the value of 06h for the FLR capability.

10.1.39 FLR_CTRL—Function Level Reset Control Register (USB EHCI—D29:F0)

Address Offset: 9Ch
Default Value: 00h
Attribute: R/W
Size: 8 bits
Function Level Reset: No

Bit	Description
7:1	Reserved
0	**Initiate FLR** — R/W. This bit is used to initiate FLR transition. A write of 1 initiates FLR transition. Since hardware must not respond to any cycles until FLR completion, the value read by software from this bit is always 0.

10.1.40 FLR_STS—Function Level Reset Status Register (USB EHCI—D29:F0)

Address Offset: 9Dh
Default Value: 00h
Attribute: RO
Size: 8 bits
Function Level Reset: No

Bit	Description
7:1	Reserved
0	**Transactions Pending (TXP)** — RO. 0 = Completions for all non-posted requests have been received. 1 = Controller has issued non-posted requests which have not been completed.

10.2 Memory-Mapped I/O Registers

The EHCI memory-mapped I/O space is composed of two sets of registers—Capability Registers and Operational Registers.

Note: Intel® Xeon® Processor D-1500 Product Family EHCI controller will not accept memory transactions (neither reads nor writes) as a target that are locked transactions. The locked transactions should not be forwarded to PCI as the address space is known to be allocated to USB.

Note: When the EHCI function is in the D3 PCI power state, accesses to the USB 2.0 memory range are ignored and result a master abort. Similarly, if the Memory Space Enable (MSE) bit (D29:F0:04h, bit 1) is not set in the Command register in configuration space, the memory range will not be decoded by Intel® Xeon® Processor D-1500 Product Family enhanced host controller (EHC). If the MSE bit is not set, Intel® Xeon® Processor D-1500 Product Family must default to allowing any memory accesses for the range specified in the BAR to go to PCI. This is because the range may not be valid and, therefore, the cycle must be made available to any other targets that may be currently using that range.

10.2.1 Host Controller Capability Registers

These registers specify the limits, restrictions and capabilities of the host controller implementation. Within the host controller capability registers, only the structural parameters register is writable. These registers are implemented in the suspend well and is only reset by the standard suspend-well hardware reset, not by HCRESET or the D3-to-D0 reset.

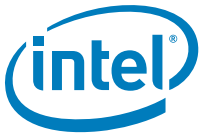
Note: The EHCI controller does not support as a target memory transactions that are locked transactions. Attempting to access the EHCI controller Memory-Mapped I/O space using locked memory transactions will result in undefined behavior.

Note: When the USB2 function is in the D3 PCI power state, accesses to the USB2 memory range are ignored and will result in a master abort. Similarly, if the Memory Space Enable (MSE) bit is not set in the Command register in configuration space, the memory range will not be decoded by the Enhanced Host Controller (EHC). If the MSE bit is not set, the EHC will not claim any memory accesses for the range specified in the BAR.

Table 10-2. Enhanced Host Controller Capability Registers

MEM_BASE + Offset	Mnemonic	Register	Default	Attribute
00h	CAPLENGTH	Capabilities Registers Length	20h	RO
02h–03h	HCIVERSION	Host Controller Interface Version Number	0100h	RO
04h–07h	HCSPARAMS	Host Controller Structural Parameters	00204208h (D29:F0) 00203206 (D26:F0)	R/W (special), RO
08h–0Bh	HCCPARAMS	Host Controller Capability Parameters	0003688h	R/W, RO

Note: "Read/Write Special" means that the register is normally read-only, but may be written when the WRT_RDONLY bit is set. Because these registers are expected to be programmed by BIOS during initialization, their contents must not get modified by HCRESET or D3-to-D0 internal reset.



10.2.1.1 CAPLENGTH—Capability Registers Length Register

Offset:	MEM_BASE + 00h	Attribute:	RO
Default Value:	20h	Size:	8 bits

Bit	Description
7:0	**Capability Register Length Value** — RO. This register is used as an offset to add to the Memory Base Register (D29:F0:10h) to find the beginning of the Operational Register Space. This field is hardwired to 20h indicating that the Operation Registers begin at offset 20h.

10.2.1.2 HCIVERSION—Host Controller Interface Version Number Register

Offset:	MEM_BASE + 02h–03h	Attribute:	RO
Default Value:	0100h	Size:	16 bits

Bit	Description
15:0	**Host Controller Interface Version Number** — RO. This is a two-byte register containing a BCD encoding of the version number of interface that this host controller interface conforms.

10.2.1.3 HCSPARAMS—Host Controller Structural Parameters

Offset:	MEM_BASE + 04h–07h	Attribute:	R/W, RO
Default Value:	00200008h (D29:F0) 00200006h (D26:F0)	Size:	32 bits

Function Level Reset: No

Note: This register is reset by a suspend well reset and not a D3-to-D0 reset or HCRESET.

Bit	Description
31:24	Reserved
23:20	**Debug Port Number (DP_N)** — RO. Hardwired to 2h indicating that the Debug Port is on the second lowest numbered port on the EHCI. EHCI#1: Port 1
19:16	Reserved
15:12	**Number of Companion Controllers (N_CC)** — RO. This field indicates the number of companion controllers associated with this USB EHCI host controller.There are no companion controllers so this field is set to zero as a read only bit.
11:8	**Number of Ports per Companion Controller (N_PCC)** — RO. This field indicates the number of ports supported per companion host controller. This field is 0h indication no other companion controller support.
7:4	Reserved. These bits are reserved and default to 0.
3:0	**N_PORTS** — R/W. This field specifies the number of physical downstream ports implemented on this host controller. The value of this field determines how many port registers are addressable in the Operational Register Space. Valid values are in the range of 1h to Fh. A 0 in this field is undefined. For Integrated USB 2.0 Rate Matching Hub Enabled: Each EHCI reports 2 ports by default. Port 0 assigned to the RMH and port 1 assigned as the debug port. When the KVM/USB-R feature is enabled it will show up as Port2 on the EHCI, and BIOS would need to update this field to 3h.

Note: This register is writable when the WRT_RDONLY bit is set.

10.2.1.4 HCCPARAMS—Host Controller Capability Parameters Register

Offset:	MEM_BASE + 08h–0Bh	Attribute:	R/W, RO
Default Value:	00036881h	Size:	32 bits

Bit	Description
31:18	Reserved
17	**Asynchronous Schedule Update Capability (ASUC)** — R/W. This bit indicates that the hardware supports the Asynch schedule prefetch enable bit in the USB command register.
16	**Periodic Schedule Update Capability (PSUC)** — R/W. This field indicates that the EHC hardware supports the Periodic Schedule prefetch bit in the USB2.0_CMD register.
15:8	**EHCI Extended Capabilities Pointer (EECP)** — RO. This field is hardwired to 68h, indicating that the EHCI capabilities list exists and begins at offset 68h in the PCI configuration space.
7:4	**Isochronous Scheduling Threshold** — R/W. This field indicates, relative to the current position of the executing host controller, where software can reliably update the isochronous schedule. When bit 7 is 0, the value of the least significant 3 bits indicates the number of micro-frames a host controller hold a set of isochronous data structures (one or more) before flushing the state. When bit 7 is a 1, then host software assumes the host controller may cache an isochronous data structure for an entire frame. Refer to the EHCI specification for details on how software uses this information for scheduling isochronous transfers. This field is hardwired to 8h.
3	Reserved
2	**Asynchronous Schedule Park Capability** — RO. This bit is hardwired to 0 indicating that the host controller does not support this optional feature
1	**Programmable Frame List Flag** — RO. 0 = System software must use a frame list length of 1024 elements with this host controller. The USB2.0_CMD register (D29:F0:CAPLENGTH + 20h, bits 3:2) *Frame List Size* field is a read-only register and must be cleared to 0. 1 = System software can specify and use a smaller frame list and configure the host controller using the USB2.0_CMD register *Frame List Size* field. The frame list must always be aligned on a 4K page boundary. This requirement ensures that the frame list is always physically contiguous.
0	**64-bit Addressing Capability** — RO. This field documents the addressing range capability of this implementation. The value of this field determines whether software should use the 32-bit or 64-bit data structures. This bit is hardwired to 1. ***Note:*** Intel® Xeon® Processor D-1500 Product Family supports 64 bit addressing only.

10.2.2 Host Controller Operational Registers

This section defines the enhanced host controller operational registers. These registers are located after the capabilities registers. The operational register base must be DWord-aligned and is calculated by adding the value in the first capabilities register (CAPLENGTH) to the base address of the enhanced host controller register address space (MEM_BASE). Since CAPLENGTH is always 20h, Table 10-3 already accounts for this offset. All registers are 32 bits in length.

Table 10-3. Enhanced Host Controller Operational Register Address Map (Sheet 1 of 2)

MEM_BASE + Offset	Mnemonic	Register Name	Default	Special Notes	Attribute
20h–23h	USB2.0_CMD	USB 2.0 Command	00080000h		R/W, RO
24h–27h	USB2.0_STS	USB 2.0 Status	00001000h		R/WC, RO
28h–2Bh	USB2.0_INTR	USB 2.0 Interrupt Enable	00000000h		R/W, RO
2Ch–2Fh	FRINDEX	USB 2.0 Frame Index	00000000h		R/W, RO
30h–33h	CTRLDSSEGMENT	Control Data Structure Segment	00000000h		R/W, RO
34h–37h	PERIODICLISTBASE	Periodic Frame List Base Address	00000000h		R/W, RO
38h–3Bh	ASYNCLISTADDR	Current Asynchronous List Address	00000000h		R/W, RO

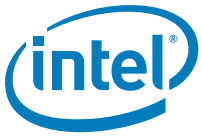


Table 10-3. Enhanced Host Controller Operational Register Address Map (Sheet 2 of 2)

MEM_BASE + Offset	Mnemonic	Register Name	Default	Special Notes	Attribute
3Ch–5Fh	—	Reserved	0h		RO
60h–63h	CONFIGFLAG	Configure Flag	00000000h	Suspend	R/W, RO
64h–67h	PORT1SC	Port 1 Status and Control	00003000h	Suspend	R/W, R/WC, RO
68h–6Bh	PORT2SC	Port 2 Status and Control	00003000h	Suspend	R/W, R/WC, RO
6Ch–6Fh	PORT3SC	Port 3 Status and Control	00003000h	Suspend	R/W, R/WC, RO
A0h–B3h	—	Debug Port Registers	Undefined		R/W, RO
B4h–3FFh	—	Reserved	Undefined		RO

Note: Software must read and write these registers using only DWord accesses.These registers are divided into two sets. The first set at offsets MEM_BASE + 00:3Bh are implemented in the core power well. Unless otherwise noted, the core well registers are reset by the assertion of any of the following:

- Core well hardware reset
- HCRESET
- D3-to-D0 reset

The second set at offsets MEM_BASE + 60h to the end of the implemented register space are implemented in the Suspend power well. Unless otherwise noted, the suspend well registers are reset by the assertion of either of the following:

- Suspend well hardware reset
- HCRESET

10.2.2.1 USB2.0_CMD—USB 2.0 Command Register

Offset: MEM_BASE + 20–23h Attribute: R/W, RO
Default Value: 00080000h Size: 32 bits

Bit	Description
31:24	Reserved
23:16	**Interrupt Threshold Control** — R/W. System software uses this field to select the maximum rate at which the host controller will issue interrupts. The only valid values are defined below. If software writes an invalid value to this register, the results are undefined. **Value** — **Maximum Interrupt Interval** 00h — Reserved 01h — 1 micro-frame 02h — 2 micro-frames 04h — 4 micro-frames 08h — 8 micro-frames (default, equates to 1 ms) 10h — 16 micro-frames (2 ms) 20h — 32 micro-frames (4 ms) 40h — 64 micro-frames (8 ms)
15:14	Reserved
13	**Asynch Schedule Update (ASC)** — R/W. This bit is used by the EHCI Asycnh schedule caching function.when operating in C0 mode. it is ignored when Asynch caching operates in Cx mode. When this bit is set, it allows the asynch schedule to be cached. When cleared, it causes the cache to be disabled and all modified entries to be written back.

Bit	Description
12	**Periodic Schedule Prefetch Enable** — R/W. This bit is used by software to enable the host controller to prefetch the periodic schedule even in C0. 0 = Pre-fetch based pause enabled only when not in C0. 1 = Pre-fetch based pause enable in C0. Once software has written a 1b to this bit to enable periodic schedule prefetching, it must disable prefetching by writing a 0b to this bit whenever periodic schedule updates are about to begin. Software should continue to dynamically disable and re-enable the prefetcher surrounding any updates to the periodic scheduler (that is, until the host controller has been reset using a HCRESET).
11:8	Unimplemented Asynchronous Park Mode Bits — RO. Hardwired to 000b indicating the host controller does not support this optional feature.
7	Light Host Controller Reset — RO. Hardwired to 0. Intel® Xeon® Processor D-1500 Product Family does not implement this optional reset.
6	**Interrupt on Async Advance Doorbell** — R/W. This bit is used as a doorbell by software to tell the host controller to issue an interrupt the next time it advances asynchronous schedule. 0 = The host controller sets this bit to a 0 after it has set the Interrupt on Async Advance status bit (D29:F0:CAPLENGTH + 24h, bit 5) in the USB2.0_STS register to a 1. 1 = Software must write a 1 to this bit to ring the doorbell. When the host controller has evicted all appropriate cached schedule state, it sets the Interrupt on Async Advance status bit in the USB2.0_STS register. If the *Interrupt on Async Advance Enable* bit in the USB2.0_INTR register (D29:F0:CAPLENGTH + 28h, bit 5) is a 1 then the host controller will assert an interrupt at the next interrupt threshold. See the EHCI specification for operational details. ***Note:*** Software should not write a 1 to this bit when the asynchronous schedule is inactive. Doing so will yield undefined results.
5	**Asynchronous Schedule Enable** — R/W. This bit controls whether the host controller skips processing the Asynchronous Schedule. 0 = Do not process the Asynchronous Schedule 1 = Use the ASYNCLISTADDR register to access the Asynchronous Schedule.
4	**Periodic Schedule Enable** — R/W. This bit controls whether the host controller skips processing the Periodic Schedule. 0 = Do not process the Periodic Schedule 1 = Use the PERIODICLISTBASE register to access the Periodic Schedule.
3:2	**Frame List Size** — RO. This field is R/W only if Programmable Frame List Flag in the HCCPARAMS registers is set to a one. This field specifies the size of the frame list. 00b = 1024 elements (4096 bytes) - Default value 01b = 512 elements (2048 bytes) 10b = 256 elements (1024 bytes) for resource constrained environments.
1	**Host Controller Reset (HCRESET)** — R/W. This control bit used by software to reset the host controller. The effects of this on root hub registers are similar to a Chip Hardware Reset (that is, RSMRST# assertion and PWROK de-assertion on Intel® Xeon® Processor D-1500 Product Family). When software writes a 1 to this bit, the host controller resets its internal pipelines, timers, counters, state machines, and so on to their initial value. Any transaction currently in progress on USB is immediately terminated. A USB reset is not driven on downstream ports. ***Note:*** PCI configuration registers and Host controller capability registers are not effected by this reset. All operational registers, including port registers and port state machines are set to their initial values. Port ownership reverts to the companion host controller(s), with the side effects described in the EHCI specification. Software must re-initialize the host controller in order to return the host controller to an operational state. This bit is cleared to 0 by the host controller when the reset process is complete. Software cannot terminate the reset process early by writing a 0 to this register. Software should not set this bit to a 1 when the HCHalted bit (D29:F0:CAPLENGTH + 24h, bit 12) in the USB2.0_STS register is a 0. Attempting to reset an actively running host controller will result in undefined behavior. This reset me be used to leave EHCI port test modes.

Bit	Description
0	**Run/Stop (RS)** — R/W. 0 = Stop (default) 1 = Run. When set to a 1, the Host controller proceeds with execution of the schedule. The Host controller continues execution as long as this bit is set. When this bit is cleared to 0, the Host controller completes the current transaction on the USB and then halts. The HCHalted bit in the USB2.0_STS register indicates when the Host controller has finished the transaction and has entered the stopped state. Software should not write a 1 to this field unless the host controller is in the Halted state (that is, HCHalted in the USBSTS register is a 1). The Halted bit is cleared immediately when the Run bit is set. The following table explains how the different combinations of Run and Halted should be interpreted: **Run/Stop** / **Halted** / **Interpretation** 0b / 0b / In the process of halting 0b / 1b / Halted 1b / 0b / Running 1b / 1b / Invalid – the HCHalted bit clears immediately Memory read cycles initiated by the EHC that receive any status other than Successful will result in this bit being cleared.

Note: The Command Register indicates the command to be executed by the serial bus host controller. Writing to the register causes a command to be executed.

10.2.2.2 USB2.0_STS—USB 2.0 Status Register

Offset:	MEM_BASE + 24h–27h	Attribute:	R/WC, RO
Default Value:	00001000h	Size:	32 bits

This register indicates pending interrupts and various states of the Host controller. The status resulting from a transaction on the serial bus is not indicated in this register. See the Interrupts description in section 4 of the EHCI specification for additional information concerning USB 2.0 interrupt conditions.

Note: For the writable bits, software must write a 1 to clear bits that are set. Writing a 0 has no effect.

Bit	Description
31:16	Reserved
15	**Asynchronous Schedule Status** — RO. This bit reports the current real status of the Asynchronous Schedule. 0 = Disabled. (Default) 1 = Enabled. ***Note:*** The Host controller is not required to *immediately* disable or enable the Asynchronous Schedule when software transitions the *Asynchronous Schedule Enable* bit (D29:F0:CAPLENGTH + 20h, bit 5) in the USB2.0_CMD register. When this bit and the *Asynchronous Schedule Enable* bit are the same value, the Asynchronous Schedule is either enabled (1) or disabled (0).
14	**Periodic Schedule Status** — RO. This bit reports the current real status of the Periodic Schedule. 0 = Disabled. (Default) 1 = Enabled. ***Note:*** The Host controller is not required to *immediately* disable or enable the Periodic Schedule when software transitions the *Periodic Schedule Enable* bit (D29:F0:CAPLENGTH + 20h, bit 4) in the USB2.0_CMD register. When this bit and the *Periodic Schedule Enable* bit are the same value, the Periodic Schedule is either enabled (1) or disabled (0).
13	**Reclamation** — RO. This read-only status bit is used to detect an empty asynchronous schedule. The operational model and valid transitions for this bit are described in Section 4 of the EHCI Specification.

Bit	Description
12	**HCHalted** — RO. 0 = This bit is a 0 when the Run/Stop bit is a 1. 1 = The Host controller sets this bit to 1 after it has stopped executing as a result of the Run/Stop bit being cleared to 0, either by software or by the Host controller hardware (such as, internal error). (Default)
11:6	Reserved
5	**Interrupt on Async Advance** — R/WC. System software can force the host controller to issue an interrupt the next time the host controller advances the asynchronous schedule by writing a 1 to the *Interrupt on Async Advance Doorbell* bit (D29:F0:CAPLENGTH + 20h, bit 6) in the USB2.0_CMD register. This bit indicates the assertion of that interrupt source.
4	**Host System Error** — R/WC. 0 = No serious error occurred during a host system access involving the Host controller module 1 = The Host controller sets this bit to 1 when a serious error occurs during a host system access involving the Host controller module. A hardware interrupt is generated to the system. Memory read cycles initiated by the EHC that receive any status other than Successful will result in this bit being set. When this error occurs, the Host controller clears the Run/Stop bit in the USB2.0_CMDregister (D29:F0:CAPLENGTH + 20h, bit 0) to prevent further execution of the scheduled TDs. A hardware interrupt is generated to the system (if enabled in the Interrupt Enable Register).
3	**Frame List Rollover** — R/WC. 0 = No *Frame List Index* rollover from its maximum value to 0. 1 = The Host controller sets this bit to a 1 when the *Frame List Index* rolls over from its maximum value to 0. Since Intel® Xeon® Processor D-1500 Product Family only supports the 1024-entry Frame List Size, the *Frame List Index* rolls over every time FRNUM13 toggles.
2	**Port Change Detect** — R/WC. This bit is allowed to be maintained in the Auxiliary power well. Alternatively, it is also acceptable that on a D3 to D0 transition of the EHCI HC device, this bit is loaded with the OR of all of the PORTSC change bits (including: Force port resume, overcurrent change, enable/disable change and connect status change). Regardless of the implementation, when this bit is readable (that is, in the D0 state), it must provide a valid view of the Port Status registers. 0 = No change bit transition from a 0 to 1 or No Force Port Resume bit transition from 0 to 1 as a result of a J-K transition detected on a suspended port. 1 = The Host controller sets this bit to 1 when any port for which the *Port Owner* bit is cleared to 0 has a change bit transition from a 0 to 1 or a Force Port Resume bit transition from 0 to 1 as a result of a J-K transition detected on a suspended port.
1	**USB Error Interrupt (USBERRINT)** — R/WC. 0 = No error condition. 1 = The Host controller sets this bit to 1 when completion of a USB transaction results in an error condition (such as, error counter underflow). If the TD on which the error interrupt occurred also had its IOC bit set, both this bit and Bit 0 are set. See the EHCI specification for a list of the USB errors that will result in this interrupt being asserted.
0	**USB Interrupt (USBINT)** — R/WC. 0 = No completion of a USB transaction whose Transfer Descriptor had its IOC bit set. No short packet is detected. 1 = The Host controller sets this bit to 1 when the cause of an interrupt is a completion of a USB transaction whose Transfer Descriptor had its IOC bit set. The Host controller also sets this bit to 1 when a short packet is detected (actual number of bytes received was less than the expected number of bytes).

10.2.2.3 USB2.0_INTR—USB 2.0 Interrupt Enable Register

Offset:	MEM_BASE + 28h–2Bh	Attribute:	R/W, RO
Default Value:	00000000h	Size:	32 bits

This register enables and disables reporting of the corresponding interrupt to the software. When a bit is set and the corresponding interrupt is active, an interrupt is generated to the host. Interrupt sources that are disabled in this register still appear in the USB2.0_STS Register to allow the software to poll for events. Each interrupt enable bit description indicates whether it is dependent on the interrupt threshold mechanism (see Section 4 of the EHCI specification), or not.

Bit	Description
31:6	Reserved
5	**Interrupt on Async Advance Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1, and the Interrupt on Async Advance bit (D29:F0:CAPLENGTH + 24h, bit 5) in the USB2.0_STS register is a 1, the host controller will issue an interrupt at the next interrupt threshold. The interrupt is acknowledged by software clearing the Interrupt on Async Advance bit.
4	**Host System Error Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1, and the Host System Error Status bit (D29:F0:CAPLENGTH + 24h, bit 4) in the USB2.0_STS register is a 1, the host controller will issue an interrupt. The interrupt is acknowledged by software clearing the Host System Error bit.
3	**Frame List Rollover Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1, and the Frame List Rollover bit (D29:F0:CAPLENGTH + 24h, bit 3) in the USB2.0_STS register is a 1, the host controller will issue an interrupt. The interrupt is acknowledged by software clearing the Frame List Rollover bit.
2	**Port Change Interrupt Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1, and the Port Change Detect bit (D29:F0:CAPLENGTH + 24h, bit 2) in the USB2.0_STS register is a 1, the host controller will issue an interrupt. The interrupt is acknowledged by software clearing the Port Change Detect bit.
1	**USB Error Interrupt Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1, and the USBERRINT bit (D29:F0:CAPLENGTH + 24h, bit 1) in the USB2.0_STS register is a 1, the host controller will issue an interrupt at the next interrupt threshold. The interrupt is acknowledged by software by clearing the USBERRINT bit in the USB2.0_STS register.
0	**USB Interrupt Enable** — R/W. 0 = Disable. 1 = Enable. When this bit is a 1, and the USBINT bit (D29:F0:CAPLENGTH + 24h, bit 0) in the USB2.0_STS register is a 1, the host controller will issue an interrupt at the next interrupt threshold. The interrupt is acknowledged by software by clearing the USBINT bit in the USB2.0_STS register.

10.2.2.4 FRINDEX—Frame Index Register

Offset:	MEM_BASE + 2Ch–2Fh	Attribute:	R/W, RO
Default Value:	00000000h	Size:	32 bits

The SOF frame number value for the bus SOF token is derived or alternatively managed from this register. Refer to Section 4 of the EHCI specification for a detailed explanation of the SOF value management requirements on the host controller. The value of FRINDEX must be within 125 µs (1 micro-frame) ahead of the SOF token value. The SOF value may be implemented as an 11-bit shadow register. For this discussion, this shadow register is 11 bits and is named SOFV. SOFV updates every 8 micro-frames (1 millisecond). An example implementation to achieve this behavior is to increment SOFV each time the FRINDEX[2:0] increments from 0 to 1.

Software must use the value of FRINDEX to derive the current micro-frame number, both for high-speed isochronous scheduling purposes and to provide the **get** micro-frame number function required to client drivers. Therefore, the value of FRINDEX and the value of SOFV must be kept consistent if chip is reset or software writes to FRINDEX. Writes to FRINDEX must also **write-through** FRINDEX[13:3] to SOFV[10:0]. In order to keep the update as simple as possible, software should never write a FRINDEX value where the three least significant bits are 111b or 000b.

Note: This register is used by the host controller to index into the periodic frame list. The register updates every 125 microseconds (once each micro-frame). Bits [12:3] are used to select a particular entry in the Periodic Frame List during periodic schedule execution. The number of bits used for the index is fixed at 10 for Intel® Xeon® Processor D-1500 Product Family since it only supports 1024-entry frame lists. This register must be written as a DWord. Word and byte writes produce undefined results. This register cannot be written unless the Host controller is in the Halted state as indicated by the *HCHalted* bit (D29:F0:CAPLENGTH + 24h, bit 12). A write to this register while the Run/Stop bit (D29:F0:CAPLENGTH + 20h, bit 0) is set to a 1 (USB2.0_CMD register) produces undefined results. Writes to this register also effect the SOF value. See Section 4 of the EHCI specification for details.

Bit	Description
31:14	Reserved
13:0	**Frame List Current Index/Frame Number** — R/W. The value in this register increments at the end of each time frame (such as, micro-frame). Bits [12:3] are used for the Frame List current index. This means that each location of the frame list is accessed 8 times (frames or micro-frames) before moving to the next index.

10.2.2.5 CTRLDSSEGMENT—Control Data Structure Segment Register

Offset:	MEM_BASE + 30h–33h	Attribute:	R/W, RO
Default Value:	00000000h	Size:	32 bits

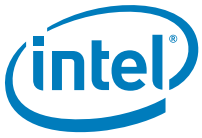
This 32-bit register corresponds to the most significant address bits [63:32] for all EHCI data structures. Since Intel® Xeon® Processor D-1500 Product Family hardwires the 64-bit Addressing Capability field in HCCPARAMS to 1, this register is used with the link pointers to construct 64-bit addresses to EHCI control data structures. This register is concatenated with the link pointer from either the PERIODICLISTBASE, ASYNCLISTADDR, or any control data structure link field to construct a 64-bit address. This register allows the host software to locate all control data structures within the same 4 GB memory segment.

Bit	Description
31:12	Upper Address[63:44] — RO. Hardwired to 0s. Intel® Xeon® Processor D-1500 Product Family EHC is only capable of generating addresses up to 16 terabytes (44 bits of address).
11:0	**Upper Address[43:32]** — R/W. This 12-bit field corresponds to address bits 43:32 when forming a control data structure address.

10.2.2.6 PERIODICLISTBASE—Periodic Frame List Base Address Register

Offset:	MEM_BASE + 34h–37h	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits

This 32-bit register contains the beginning address of the Periodic Frame List in the system memory. Since Intel® Xeon® Processor D-1500 Product Family host controller operates in 64-bit mode (as indicated by the 1 in the 64-bit Addressing Capability field in the HCCSPARAMS register) (offset 08h, bit 0), then the most significant 32 bits of every control data structure address comes from the CTRLDSSEGMENT register. HCD loads this register prior to starting the schedule execution by the host controller. The



memory structure referenced by this physical memory pointer is assumed to be 4-Kbyte aligned. The contents of this register are combined with the Frame Index Register (FRINDEX) to enable the Host controller to step through the Periodic Frame List in sequence.

Bit	Description
31:12	**Base Address (Low)** — R/W. These bits correspond to memory address signals 31:12, respectively.
11:0	Reserved

10.2.2.7 ASYNCLISTADDR—Current Asynchronous List Address Register

Offset:	MEM_BASE + 38h–3Bh	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits

This 32-bit register contains the address of the next asynchronous queue head to be executed. Since Intel® Xeon® Processor D-1500 Product Family host controller operates in 64-bit mode (as indicated by a 1 in 64-bit Addressing Capability field in the HCCPARAMS register) (offset 08h, bit 0), then the most significant 32 bits of every control data structure address comes from the CTRLDSSEGMENT register (offset 08h). Bits [4:0] of this register cannot be modified by system software and will always return 0s when read. The memory structure referenced by this physical memory pointer is assumed to be 32-byte aligned.

Bit	Description
31:5	**Link Pointer Low (LPL)** — R/W. These bits correspond to memory address signals 31:5, respectively. This field may only reference a Queue Head (QH).
4:0	Reserved

10.2.2.8 CONFIGFLAG—Configure Flag Register

Offset:	MEM_BASE + 60h–63h	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits

This register is in the suspend power well. It is only reset by hardware when the suspend power is initially applied or in response to a host controller reset.

Bit	Description
31:1	Reserved
0	**Configure Flag (CF)** — R/W. Host software sets this bit as the last action in its process of configuring the Host controller. This bit controls the default port-routing control logic. Bit values and side-effects are listed below. See Chapter 4 of the EHCI specification for operation details. 0 = Compatibility debug only (default). 1 = Port routing control logic default-routes all ports to this host controller.

10.2.2.9 PORTSC—Port N Status and Control Register

Offset: Port 0 RMH: MEM_BASE + 64h–67h
Port 1 Debug Port: MEM_BASE + 68–6Bh
Port 2 USB redirect (if enabled): MEM_BASE + 6C–6Fh

Attribute: R/W, R/WC, RO
Default Value: 00003000h Size: 32 bits

Note: This register is associated with the upstream ports of the EHCI controller and does not represent downstream hub ports. USB Hub class commands must be used to determine RMH port status and enable test modes. See Chapter 11 of the USB Specification, Revision 2.0 for more details. Rate Matching Hub wake capabilities can be configured by the RMHWKCTL Register (RCBA+35B0h) located in the Chipset Configuration chapter.

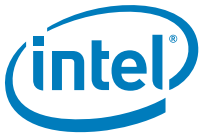
A host controller must implement one or more port registers. Software uses the N_Port information from the Structural Parameters Register to determine how many ports need to be serviced. All ports have the structure defined below. Software must not write to unreported Port Status and Control Registers.

This register is in the suspend power well. It is only reset by hardware when the suspend power is initially applied or in response to a host controller reset. The initial conditions of a port are:

- No device connected
- Port disabled.

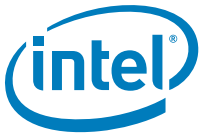
When a device is attached, the port state transitions to the attached state and system software will process this as with any status change notification. Refer to Section 4 of the EHCI specification for operational requirements for how change events interact with port suspend mode.

Bit	Description
31:23	Reserved
22	**Wake on Overcurrent Enable (WKOC_E)** — R/W. 0 = Disable. (Default) 1 = Enable. Writing this bit to a 1 enables the setting of the PME Status bit in the Power Management Control/Status Register (offset 54, bit 15) when the overcurrent Active bit (bit 4 of this register) is set.
21	**Wake on Disconnect Enable (WKDSCNNT_E)** — R/W. 0 = Disable. (Default) 1 = Enable. Writing this bit to a 1 enables the setting of the PME Status bit in the Power Management Control/Status Register (offset 54, bit 15) when the Current Connect Status changes from connected to disconnected (that is, bit 0 of this register changes from 1 to 0).
20	**Wake on Connect Enable (WKCNNT_E)** — R/W. 0 = Disable. (Default) 1 = Enable. Writing this bit to a 1 enables the setting of the PME Status bit in the Power Management Control/Status Register (offset 54, bit 15) when the Current Connect Status changes from disconnected to connected (that is, bit 0 of this register changes from 0 to 1).



Bit	Description
19:16	**Port Test Control** — R/W. When this field is 0s, the port is NOT operating in a test mode. A non-zero value indicates that it is operating in test mode and the specific test mode is indicated by the specific value. The encoding of the test mode bits are (0110b – 1111b are reserved): **Value** — **Maximum Interrupt Interval** 0000b — Test mode not enabled (default) 0001b — Test J_STATE 0010b — Test K_STATE 0011b — Test SE0_NAK 0100b — Test Packet 0101b — FORCE_ENABLE Refer to the USB Specification Revision 2.0, Chapter 7 for details on each test mode.
15:14	Reserved
13	**Port Owner** — R/W. This bit unconditionally goes to a 0 when the Configured Flag bit in the USB2.0_CMD register makes a 0 to 1 transition. System software uses this field to release ownership of the port to a selected host controller (in the event that the attached device is not a high-speed device). Software writes a 1 to this bit when the attached device is not a high-speed device. A 1 in this bit means that a companion host controller owns and controls the port. See Section 4 of the EHCI Specification for operational details.
12	**Port Power (PP)** — RO. Read-only with a value of 1. This indicates that the port does have power.
11:10	**Line Status**— RO.These bits reflect the current logical levels of the D+ (bit 11) and D– (bit 10) signal lines. These bits are used for detection of low-speed USB devices prior to the port reset and enable sequence. This field is valid only when the port enable bit is 0 and the current connect status bit is set to a 1. 00 = SE0 10 = J-state 01 = K-state 11 = Undefined
9	Reserved
8	**Port Reset** — R/W. When software writes a 1 to this bit (from a 0), the bus reset sequence as defined in the USB Specification, Revision 2.0 is started. Software writes a 0 to this bit to terminate the bus reset sequence. Software must keep this bit at a 1 long enough to ensure the reset sequence completes as specified in the USB Specification, Revision 2.0. 1 = Port is in Reset. 0 = Port is not in Reset. ***Note:*** When software writes a 0 to this bit, there may be a delay before the bit status changes to a 0. The bit status will not read as a 0 until after the reset has completed. If the port is in high-speed mode after reset is complete, the host controller will automatically enable this port (such as, set the *Port Enable* bit to a 1). A host controller must terminate the reset and stabilize the state of the port within 2 milliseconds of software transitioning this bit from 0 to 1. For example: if the port detects that the attached device is high-speed during reset, then the host controller must have the port in the enabled state within 2 ms of software writing this bit to a 0. The HCHalted bit (D29:F0:CAPLENGTH + 24h, bit 12) in the USB2.0_STS register should be a 0 before software attempts to use this bit. The host controller may hold Port Reset asserted to a 1 when the HCHalted bit is a 1. This bit is 0 if Port Power is 0. ***Note:*** System software should not attempt to reset a port if the *HCHalted* bit in the USB2.0_STS register is a 1. Doing so will result in undefined behavior.

Bit	Description
7	**Suspend** — R/W. 0 = Port not in suspend state.(Default) 1 = Port in suspend state. Port Enabled Bit and Suspend bit of this register define the port states as follows: **Port Enabled** / **Suspend** / **Port State** 0 / X / Disabled 1 / 0 / Enabled 1 / 1 / Suspend When in suspend state, downstream propagation of data is blocked on this port, except for port reset. The bit status does not change until the port is suspended and that there may be a delay in suspending a port depending on the activity on the port. The host controller will unconditionally set this bit to a 0 when software sets the *Force Port Resume* bit to a 0 (from a 1). A write of 0 to this bit is ignored by the host controller. If host software sets this bit to a 1 when the port is not enabled (that is, Port enabled bit is a 0), the results are undefined.
6	**Force Port Resume** — R/W. 0 = No resume (K-state) detected/driven on port. (Default) 1 = Resume detected/driven on port. Software sets this bit to a 1 to drive resume signaling. The Host controller sets this bit to a 1 if a J-to-K transition is detected while the port is in the Suspend state. When this bit transitions to a 1 because a J-to-K transition is detected, the Port Change Detect bit (D29:F0:CAPLENGTH + 24h, bit 2) in the USB2.0_STS register is also set to a 1. If software sets this bit to a 1, the host controller must not set the Port Change Detect bit. ***Note:*** When the EHCI controller owns the port, the resume sequence follows the defined sequence documented in the USB Specification, Revision 2.0. The resume signaling (Full-speed 'K') is driven on the port as long as this bit remains a 1. Software must appropriately time the Resume and set this bit to a 0 when the appropriate amount of time has elapsed. Writing a 0 (from 1) causes the port to return to high-speed mode (forcing the bus below the port into a high-speed idle). This bit will remain a 1 until the port has switched to the high-speed idle.
5	**Overcurrent Change** — R/WC. The functionality of this bit is not dependent upon the port owner. Software clears this bit by writing a 1 to it. 0 = No change. (Default) 1 = There is a change to Overcurrent Active.
4	**Overcurrent Active** — RO. 0 = This port does not have an overcurrent condition. (Default) 1 = This port currently has an overcurrent condition. This bit will automatically transition from 1 to 0 when the over current condition is removed. Intel® Xeon® Processor D-1500 Product Family automatically disables the port when the overcurrent active bit is 1.
3	**Port Enable/Disable Change** — R/WC. For the root hub, this bit gets set to a 1 only when a port is disabled due to the appropriate conditions existing at the EOF2 point (See Chapter 11 of the USB Specification for the definition of a port error). This bit is not set due to the Disabled-to-Enabled transition, nor due to a disconnect. Software clears this bit by writing a 1 to it. 0 = No change in status. (Default). 1 = Port enabled/disabled status has changed.
2	**Port Enabled/Disabled** — R/W. Ports can only be enabled by the host controller as a part of the reset and enable. Software cannot enable a port by writing a 1 to this bit. Ports can be disabled by either a fault condition (disconnect event or other fault condition) or by host software. The bit status does not change until the port state actually changes. There may be a delay in disabling or enabling a port due to other host controller and bus events. 0 = Disable 1 = Enable (Default)
1	**Connect Status Change** — R/WC. This bit indicates a change has occurred in the port's Current Connect Status. Software sets this bit to 0 by writing a 1 to it. 0 = No change (Default). 1 = Change in Current Connect Status. The host controller sets this bit for all changes to the port device connect status, even if system software has not cleared an existing connect status change. For example, the insertion status changes twice before system software has cleared the changed condition, hub hardware will be "setting" an already-set bit (that is, the bit will remain set).
0	**Current Connect Status** — RO. This value reflects the current state of the port, and may not correspond directly to the event that caused the Connect Status Change bit (Bit 1) to be set. 0 = No device is present. (Default) 1 = Device is present on port.



10.2.3 USB 2.0-Based Debug Port Registers

The Debug port's registers are located in the same memory area, defined by the Base Address Register (MEM_BASE), as the standard EHCI registers. The base offset for the debug port registers (A0h) is declared in the Debug Port Base Offset Capability Register at Configuration offset 5Ah (D29:F0:offset 5Ah). The specific EHCI port that supports this debug capability (Port 1 for D29:F0) is indicated by a 4-bit field (bits 20–23) in the HCSPARAMS register of the EHCI controller. The address map of the Debug Port registers is shown in Table 10-4.

Table 10-4. Debug Port Register Address Map

MEM_BASE + Offset	Mnemonic	Register Name	Default	Attribute
A0–A3h	CNTL_STS	Control / Status	00000000h	R/W, R/WC, RO
A4–A7h	USBPID	USB PIDs	00000000h	R/W, RO
A8–AFh	DATABUF[7:0]	Data Buffer (Bytes 7:0)	00000000 00000000h	R/W
B0–B3h	CONFIG	Configuration	00007F01h	R/W

Notes:
1. All of these registers are implemented in the core well and reset by PLTRST#, EHC HCRESET, and a EHC D3-to-D0 transition.
2. The hardware associated with this register provides no checks to ensure that software programs the interface correctly. How the hardware behaves when programmed improperly is undefined.

10.2.3.1 CNTL_STS—Control / Status Register

Offset:	MEM_BASE + A0h	Attribute:	R/W, R/WC, RO
Default Value:	00000000h	Size:	32 bits
Power well:	Suspend		

Bit	Description
31	Reserved
30	**OWNER_CNT —** R/W. 0 = Ownership of the debug port is NOT forced to the EHCI controller (Default) 1 = Ownership of the debug port is forced to the EHCI controller (that is, immediately taken away from the companion Classic USB Host controller) If the port was already owned by the EHCI controller, then setting this bit has no effect. This bit overrides all of the ownership-related bits in the standard EHCI registers.
29	Reserved
28	**ENABLED_CNT —** R/W. 0 = Software can clear this by writing a 0 to it. The hardware clears this bit for the same conditions where the Port Enable/Disable Change bit (in the PORTSC register) is set. (Default) 1 = Debug port is enabled for operation. Software can directly set this bit if the port is already enabled in the associated PORTSC register (this is enforced by the hardware).
27:17	Reserved
16	**DONE_STS —** R/WC. Software can clear this by writing a 1 to it. 0 = Request Not complete 1 = Set by hardware to indicate that the request is complete.
15:12	**LINK_ID_STS —** RO. This field identifies the link interface. 0h = Hardwired. Indicates that it is a USB Debug Port.
11	Reserved
10	**IN_USE_CNT —** R/W. Set by software to indicate that the port is in use. Cleared by software to indicate that the port is free and may be used by other software. This bit is cleared after reset. (This bit has no affect on hardware.)

Bit	Description
9:7	**EXCEPTION_STS —** RO. This field indicates the exception when the ERROR_GOOD#_STS bit is set. This field should be ignored if the ERROR_GOOD#_STS bit is 0. 000 =No Error. (Default) **Note:** This should not be seen since this field should only be checked if there is an error. 0 = 001 =Transaction error: Indicates the USB 2.0 transaction had an error (CRC, bad PID, timeout, and so on) 0 = 010 =Hardware error. Request was attempted (or in progress) when port was suspended or reset. All Other combinations are reserved.
6	**ERROR_GOOD#_STS —** RO. 0 = Hardware clears this bit to 0 after the proper completion of a read or write. (Default) 1 = Error has occurred. Details on the nature of the error are provided in the Exception field.
5	**GO_CNT** — R/W. 0 = Hardware clears this bit when hardware sets the DONE_STS bit. (Default) 1 = Causes hardware to perform a read or write request. ***Note:*** Writing a 1 to this bit when it is already set may result in undefined behavior.
4	**WRITE_READ#_CNT —** R/W. Software clears this bit to indicate that the current request is a read. Software sets this bit to indicate that the current request is a write. 0 = Read (Default) 1 = Write
3:0	**DATA_LEN_CNT —** R/W. This field is used to indicate the size of the data to be transferred. default = 0h. For write operations, this field is set by software to indicate to the hardware how many bytes of data in Data Buffer are to be transferred to the console. A value of 0h indicates that a zero-length packet should be sent. A value of 1–8 indicates 1–8 bytes are to be transferred. Values 9–Fh are invalid and how hardware behaves if used is undefined. For read operations, this field is set by hardware to indicate to software how many bytes in Data Buffer are valid in response to a read operation. A value of 0h indicates that a zero length packet was returned and the state of Data Buffer is not defined. A value of 1–8 indicates 1–8 bytes were received. Hardware is not allowed to return values 9–Fh. The transferring of data always starts with byte 0 in the data area and moves toward byte 7 until the transfer size is reached.

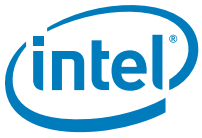
Notes:
1. Software should do Read-Modify-Write operations to this register to preserve the contents of bits not being modified. This include Reserved bits.
2. To preserve the usage of RESERVED bits in the future, software should always write the same value read from the bit until it is defined. Reserved bits will always return 0 when read.

10.2.3.2 USBPID—USB PIDs Register

Offset:	MEM_BASE + A4h–A7h	Attribute:	R/W, RO
Default Value:	00000000h	Size:	32 bits
Power well:	Suspend		

This DWord register is used to communicate PID information between the USB debug driver and the USB debug port. The debug port uses some of these fields to generate USB packets, and uses other fields to return PID information to the USB debug driver.

Bit	Description
31:24	Reserved
23:16	**RECEIVED_PID_STS[23:16]** — RO. Hardware updates this field with the received PID for transactions in either direction. When the controller is writing data, this field is updated with the handshake PID that is received from the device. When the host controller is reading data, this field is updated with the data packet PID (if the device sent data), or the handshake PID (if the device NAKs the request). This field is valid when the hardware clears the GO_DONE#_CNT bit.
15:8	**SEND_PID_CNT[15:8]** — R/W. Hardware sends this PID to begin the data packet when sending data to USB (that is, WRITE_READ#_CNT is asserted). Software typically sets this field to either DATA0 or DATA1 PID values.
7:0	**TOKEN_PID_CNT[7:0]** — R/W. Hardware sends this PID as the Token PID for each USB transaction. Software typically sets this field to either IN, OUT, or SETUP PID values.



10.2.3.3 DATABUF[7:0]—Data Buffer Bytes[7:0] Register

Offset:	MEM_BASE + A8h–AFh	Attribute:	R/W
Default Value:	0000000000000000h	Size:	64 bits

This register can be accessed as 8 separate 8-bit registers or 2 separate 32-bit register.

Bit	Description
63:0	**DATABUFFER[63:0]** — R/W. This field is the 8 bytes of the data buffer. Bits 7:0 correspond to least significant byte (byte 0). Bits 63:56 correspond to the most significant byte (byte 7). The bytes in the Data Buffer must be written with data before software initiates a write request. For a read request, the Data Buffer contains valid data when DONE_STS bit (offset A0, bit 16) is cleared by the hardware, ERROR_GOOD#_STS (offset A0, bit 6) is cleared by the hardware, and the DATA_LENGTH_CNT field (offset A0, bits 3:0) indicates the number of bytes that are valid.

10.2.3.4 CONFIG—Configuration Register

Offset:	MEM_BASE + B0–B3h	Attribute:	R/W
Default Value:	00007F01h	Size:	32 bits

Bit	Description
31:15	Reserved
14:8	**USB_ADDRESS_CNF** — R/W. This 7-bit field identifies the USB device address used by the controller for all Token PID generation. (Default = 7Fh)
7:4	Reserved
3:0	**USB_ENDPOINT_CNF** — R/W. This 4-bit field identifies the endpoint used by the controller for all Token PID generation. (Default = 1h)

§

11 xHCI Controller Registers (D20:F0)

11.1 USB xHCI Configuration Registers (USB xHCI—D20:F0)

Note: Register address locations that are not shown in Table 11-1 should be treated as Reserved (see Section 4.2 for details).

Note: "Multiple" in the Power Well column means that multiple power wells apply to this register since the individual fields in the register may be on different power wells.

Table 11-1. USB xHCI PCI Register Address Map (USB xHCI—D20:F0) (Sheet 1 of 2)

Offset	Power Well	Mnemonic	Register Name	Default Value	Type
00h–01h	Core	VID	Vendor Identification	8086h	RO
02h–03h	Core	DID	Device Identification	See register description	RO
04h–05h	Core	PCICMD	PCI Command	0000h	R/W, RO
06h–07h	Core	PCISTS	PCI Status	0290h	R/WC, RO
08h	Core	RID	Revision Identification	00h	RO
09h	Core	PI	Programming Interface	30h	RO
0Ah	Core	SCC	Sub Class Code	03h	RO
0Bh	Core	BCC	Base Class Code	0Ch	RO
0Dh	Core	PMLT	Primary Master Latency Timer	00h	RO
0Eh	Core	HEADTYP	Header Type	00h	RO
10h–13h	Core	MEM_BASE_L	Memory Base Address Low	00000004h	R/W, RO
14h–17h	Core	MEM_BASE_H	Memory Base Address High	00000000h	R/W
2Ch–2Dh	Core	SVID	USB xHCI Subsystem Vendor Identification	0000h	R/W
2Eh–2Fh	Core	SID	USB xHCI Subsystem Identification	0000h	R/W
34h	Core	CAP_PTR	Capabilities Pointer	70h	RO
3Ch	Core	INT_LN	Interrupt Line	00h	R/W
3Dh	Core	INT_PN	Interrupt Pin	See register description	RO
40h–43h	Core	XHCC	xHC System Bus Configuration	0000F0FDh	R/W, R/WC
44h–47h	Multiple	XHCC2	xHC System Bus Configuration 2	00000000h	R/WO
60h	Sus	SBRN	Serial Bus Release Number	30h	RO
61h	Multiple	FL_ADJ	Frame Length Adjustment	20h	R/W
70h	Core	PWR_CAPID	PCI Power Management Capability ID	01h	RO
71h	Core	NXT_PTR1	Next Item Pointer #1	80h	R/W
72h–73h	Core	PWR_CAP	Power Management Capabilities	C9C2h	R/W, RO
74h–75h	Multiple	PWR_CNTL_STS	Power Management Control / Status	0000h	R/W, R/WC, RO
80h	Core	MSI_CAPID	Message Signaled Interrupt Capability ID	05h	RO

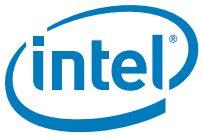


Table 11-1. USB xHCI PCI Register Address Map (USB xHCI—D20:F0) (Sheet 2 of 2)

Offset	Power Well	Mnemonic	Register Name	Default Value	Type
81h	Core	NXT_PTR2	Next Item Pointer #2	00h	RO
82h–83h	Core	MSI_MCTL	MSI Message Control Register	0086h	RO, R/W
84h–87h	Core	MSI_LMAD	MSI Lower Message Address	00000000h	RW, RO
88h–8Bh	Core	MSI_UMAD	MSI Upper Message Address	000000h	R/W
8Ch–8Fh	Core	MSI_MD	MSI Message Data	00000000h	R/W
C0h–C3h	Sus	U2OCM1	XHCI USB2 Overcurrent Pin Mapping 1	00000000h	R/W, RO
C4h–C7h	Sus	U2OCM2	XHCI USB2 Overcurrent Pin Mapping 2	00000000h	R/W, RO
C8h–CBh	Sus	U3OCM1	XHCI USB3 Overcurrent Pin Mapping 1	00000000h	R/W, RO
CCh–CFh	Sus	U3OCM2	XHCI USB3 Overcurrent Pin Mapping 2	00000000h	R/W, RO
D0h–D3h	Multiple	XUSB2PR	xHC USB 2.0 Port Routing	00000000h	R/W, RO
D4h–D7h	Core	XUSB2PRM	xHC USB 2.0 Port Routing Mask	00000000h	RO, R/WLO
D8h–dBh		USB3_PSSEN	USB 3.0 Port SuperSpeed Enable Register	00000000h	RO, R/W
D8h–dBh	Multiple	USB3PR	USB3 Port Routing	00000000h	R/W, RO
DCh–DFh	Core	USB3PRM	USB 3.0 Port Routing Mask	00000000h	R/W, RO
E4h–E7h	Multiple	USB2PDO	USB2 Port Disable Override	00000000h	R/WO
E8h–EBh	Multiple	USB3PDO	USB3 Port Disable Override	00000000h	R/WO

11.2 VID—Vendor Identification Register (USB xHCI—D20:F0)

Offset Address: 00h–01h
Attribute: RO
Default Value: 8086h
Size: 16 bits

Bit	Description
15:0	**Vendor ID** — RO. This is a 16-bit value assigned to Intel.

11.2.1 DID—Device Identification Register (USB xHCI—D20:F0)

Offset Address: 02h–03h
Attribute: RO
Default Value: See bit description
Size: 16 bits

Bit	Description
15:0	**Device ID** — RO. This is a 16-bit value assigned to Intel® Xeon® Processor D-1500 Product Family USB xHCI controller.

11.2.2 PCICMD—PCI Command Register (USB xHCI—D20:F0)

Address Offset: 04h–05h
Attribute: R/W, RO
Default Value: 0000h
Size: 16 bits

Bit	Description
15:11	Reserved
10	**Interrupt Disable** — R/W. 0 = The function is capable of generating interrupts. 1 = The function can not generate its interrupt to the interrupt controller. The corresponding Interrupt Status bit (D20:F0, Offset 06h, bit 3) is not affected by the interrupt enable.

Bit	Description
9	Fast Back to Back Enable (FBE) — RO. Hardwired to 0.
8	**SERR# Enable (SERR_EN)** — R/W. 0 = Disables xHC's capability to generate an SERR#. 1 = The xHCI Host controller (xHC) is capable of generating (internally) SERR# in the following cases: — When it receive a completion status other than "successful" for one of its DMA initiated memory reads on its internal interface. — When it detects an address or command parity error and the Parity Error Response bit is set. — When it detects a data parity error (when the data is going into the xHC) and the Parity Error Response bit is set.
7	Wait Cycle Control (WCC) — RO. Hardwired to 0.
6	**Parity Error Response (PER)** — R/W. 0 = The xHC is not checking for correct parity (on its internal interface). 1 = The xHC is checking for correct parity (on its internal interface) and halt operation when bad parity is detected during the data phase. ***Note:*** This applies to both requests and completions from the system interface. This bit must be set in order for the parity errors to generate SERR#.
5	VGA Palette Snoop (VPS) — RO. Hardwired to 0.
4	Postable Memory Write Enable (PMWE) — RO. Hardwired to 0.
3	Special Cycle Enable (SCE) — RO. Hardwired to 0.
2	**Bus Master Enable (BME)** — R/W. 0 = Disables this functionality. 1 = Enables the xHC to act as a master on the PCI bus for USB transfers.
1	**Memory Space Enable (MSE)** — R/W. This bit controls access to the xHC Memory Space registers. 0 = Disables this functionality. 1 = Enables accesses to the xHC Memory Space registers. The Base Address register (D20:F0:10h) should be programmed before this bit is set.
0	I/O Space Enable (IOSE) — RO. Hardwired to 0.

11.2.3 PCISTS—PCI Status Register (USB xHCI—D20:F0)

Address Offset:	06h–07h	Attribute:	R/WC, RO
Default Value:	0290h	Size:	16 bits

Note: For the writable bits, software must write a 1 to clear bits that are set. Writing a 0 to the bit has no effect.

Bit	Description
15	**Detected Parity Error (DPE)** — R/WC. 0 = No parity error detected. 1 = This bit is set by Intel® Xeon® Processor D-1500 Product Family when a parity error is seen by the xHCI controller, regardless of the setting of bit 6 or bit 8 in the Command register or any other conditions.
14	**Signaled System Error (SSE)** — R/WC. 0 = No SERR# signaled by Intel® Xeon® Processor D-1500 Product Family. 1 = This bit is set by Intel® Xeon® Processor D-1500 Product Family when it signals SERR# (internally). The SER_EN bit (bit 8 of the Command Register) must be 1 for this bit to be set.
13	**Received Master Abort (RMA)** — R/WC. 0 = No master abort received by xHC on a memory access. 1 = This bit is set when xHC, as a master, receives a master abort status on a memory access. This is treated as a Host Error and halts the DMA engines. This event can optionally generate an SERR# by setting the SERR# Enable bit.
12	**Received Target Abort (RTA)** — R/WC. 0 = No target abort received by xHC on memory access. 1 = This bit is set when xHC, as a master, receives a target abort status on a memory access. This is treated as a Host Error and halts the DMA engines. This event can optionally generate an SERR# by setting the SERR# Enable bit.
11	Signaled Target Abort (STA) — RO. This bit is used to indicate when the xHCI function responds to a cycle with a target abort. There is no reason for this to happen, so this bit is hardwired to 0.

Bit	Description
10:9	DEVSEL# Timing Status (DEVT_STS) — RO. This 2-bit field defines the timing for DEVSEL# assertion.
8	**Master Data Parity Error Detected (DPED)** — R/WC. 0 = No data parity error detected on USB read completion packet. 1 = This bit is set by Intel® Xeon® Processor D-1500 Product Family when a data parity error is detected on a xHC read completion packet on the internal interface to the xHCI host controller and bit 6 of the Command register is set to 1.
7	Fast Back to Back Capable (FB2BC) — RO. Hardwired to 1.
6	User Definable Features (UDF) — RO. Hardwired to 0.
5	66 MHz Capable (66 MHz _CAP) — RO. Hardwired to 0.
4	Capabilities List (CAP_LIST) — RO. Hardwired to 1 indicating that offset 34h contains a valid capabilities pointer.
3	**Interrupt Status** — RO. This bit reflects the state of this function's interrupt at the input of the enable/disable logic. 0 = This bit will be 0 when the interrupt is de-asserted. 1 = This bit is a 1 when the interrupt is asserted. The value reported in this bit is independent of the value in the Interrupt Enable bit.
2:0	Reserved

11.2.4 RID—Revision Identification Register (USB xHCI—D20:F0)

Offset Address: 08h Attribute: RO
Default Value: See bit description Size: 8 bits

Bit	Description
7:0	**Revision ID** — RO. This field indicates the device specific revision identifier.

11.2.5 PI—Programming Interface Register (USB xHCI—D20:F0)

Address Offset: 09h Attribute: RO
Default Value: 30h Size: 8 bits

Bit	Description
7:0	**Programming Interface** — RO. A value of 30h indicates that this USB host controller conforms to the xHCI Specification.

11.2.6 SCC—Sub Class Code Register (USB xHCI—D20:F0)

Address Offset: 0Ah Attribute: RO
Default Value: 03h Size: 8 bits

Bit	Description
7:0	**Sub Class Code (SCC)** — RO. 03h = Universal Serial Bus host controller.

11.2.7 BCC—Base Class Code Register (USB xHCI—D20:F0)

Address Offset: 0Bh Attribute: RO
Default Value: 0Ch Size: 8 bits

Bit	Description
7:0	**Base Class Code (BCC)** — RO. 0Ch = Serial bus controller.

11.2.8 PMLT—Primary Master Latency Timer Register (USB xHCI—D20:F0)

Address Offset: 0Dh
Default Value: 00h
Attribute: RO
Size: 8 bits

Bit	Description
7:0	**Master Latency Timer Count (MLTC)** — RO. Hardwired to 00h. Because the xHCI controller is internally implemented with arbitration on an interface (and not PCI), it does not need a master latency timer.

11.2.9 HEADTYP—Header Type Register (USB xHCI—D20:F0)

Address Offset: 0Eh
Default Value: 00h
Attribute: RO
Size: 8 bits

Bit	Description
7	**Multi-Function Device** — RO. When set to '1' indicates this is a multifunction device: 0 = Single-function device 1 = Multi-function device.
6:0	Configuration Layout. Hardwired to 00h, which indicates the standard PCI configuration layout.

11.2.10 MEM_BASE_L—Memory Base Address Low Register (USB xHCI—D20:F0)

Address Offset: 10h–13h
Default Value: 00000004h
Attribute: R/W, RO
Size: 32 bits

Bit	Description
31:16	**Base Address** — R/W. Bits [31:16] correspond to memory address signals [31:16], respectively. This gives 64 KB of relocatable memory space aligned to 64 KB boundaries.
15:4	Reserved
3	**Prefetchable** — RO. Hardwired to 0 indicating that this range should not be prefetched.
2:1	**Type** — RO. Hardwired to 10 indicating that this range can be mapped anywhere within 64-bit address space.
0	**Resource Type Indicator (RTE)** — RO. Hardwired to 0 indicating that the base address field in this register maps to memory space.

11.2.11 MEM_BASE_H—Memory Base Address High Register (USB xHCI—D20:F0)

Address Offset: 14h–17h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits

Bit	Description
31:0	**Base Address** — R/W. Bits [63:32] correspond to memory address signals [63:32], respectively. This gives 64 KB of relocatable memory space aligned to 64 KB boundaries.

11.2.12 SVID—USB xHCI Subsystem Vendor ID Register (USB xHCI—D20:F0)

Address Offset: 2Ch–2Dh
Default Value: 0000h
Reset: None
Attribute: R/W
Size: 16 bits

Bit	Description
15:0	**Subsystem Vendor ID (SVID)** — R/W. This register, in combination with the xHC Subsystem ID register, enables the operating system to distinguish each subsystem from the others.

11.2.13 SID—USB xHCI Subsystem ID Register (USB xHCI—D20:F0)

Address Offset: 2Eh–2Fh
Default Value: 0000h
Reset: None
Attribute: R/W
Size: 16 bits

Bit	Description
15:0	**Subsystem ID (SID)** — R/W. BIOS sets the value in this register to identify the Subsystem ID. This register, in combination with the Subsystem Vendor ID register, enables the operating system to distinguish each subsystem from other(s).

11.2.14 CAP_PTR—Capabilities Pointer Register (USB xHCI—D20:F0)

Address Offset: 34h
Default Value: 70h
Attribute: RO
Size: 8 bits

Bit	Description
7:0	**Capabilities Pointer (CAP_PTR)** — RO. This register points to the starting offset of the xHC capabilities ranges.

11.2.15 INT_LN—Interrupt Line Register (USB xHCI—D20:F0)

Address Offset: 3Ch
Default Value: 00h
Function Level Reset: No
Attribute: R/W
Size: 8 bits

Bit	Description
7:0	**Interrupt Line (INT_LN)** — R/W. This data is not used by Intel® Xeon® Processor D-1500 Product Family. It is used as a scratchpad register to communicate to software the interrupt line that the interrupt pin is connected to.

11.2.16 INT_PN—Interrupt Pin Register (USB xHCI—D20:F0)

Address Offset: 3Dh
Default Value: See Description
Attribute: RO
Size: 8 bits

Bit	Description
7:0	**Interrupt Pin** — RO. Bits 3:0 reflect the value of the interrupt pin registers in chipset configuration space. Bits 7:4 are always 0h

11.2.17 XHCC—xHC System Bus Configuration Register (USB xHCI—D20:F0)

Address Offset: 40-43h Attribute: R/W, R/WC
Default Value: 0000F0FDh Size: 32 bits

Bit	Description
31:25	Reserved
24	**Master/Target Abort SERR (RMTASERR)** — R/W. When set, this bit allows the out-of-band error reporting from the xHCI Controller to be reported as SERR# (if SERR# reporting is enabled) and thus setting the STS.SSE bit.
23	**Unsupported Request Detected (URD)** — R/WC. This bit is set by HW when the xHCI Controller received an unsupported request posted cycle. Once set, this bit is cleared by SW.
22	**Unsupported Request Report Enable (URRE)** — R/W. When set, this bit allows the URD bit to be reported as SERR# (if SERR# reporting is enabled) and thus setting the STS.SSE bit.
21:19	**Inactivity Initiated L1 Enable (IIL1E)** — R/W. If programmed to a non-zero value, the bit field allows L1 power management to be enabled after the time-out period specified. 000 = Disabled 001 = 32 bb_cclk 010 = 64 bb_cclk 011 = 128 bb_cclk 100 = 256 bb_cclk 101 = 512 bb_cclk 110 = 1024 bb_cclk 111 = 131072 bb_cclk
18	**xHC Initiated L1 Enable (XHCIL1E)** — R/W. 0 = xHC-initiated L1 power management is disabled 1 = Allows xHC-initiated L1 power management to be enabled
17	**D3 Initiated L1 Enable (D3IL1E)** — R/W. 0 = PCI device state D3-initiated L1 power management is disabled 1 = Allows PCI device state D3-initiated L1 power management to be enabled
16:0	Reserved

11.2.18 XHCC2—xHC System Bus Configuration Register 2 (USB xHCI—D20:F0)

Address Offset: 44-47h Attribute: R/WO
Default Value: 00000000h Size: 32 bits

Bit	Description
31	**OC Configuration Done (OCCFDONE)** — R/WO. This bit is used by BIOS to prevent spurious switching during OC configuration. ***Note:*** This bit must be set by BIOS after configuration of the OC mapping bits is complete. Once this bit is set, OC mapping shall not be changed by SW.
30:0	Reserved

11.2.19 SBRN—Serial Bus Release Number Register (USB xHCI—D20:F0)

Address Offset: 60h Attribute: RO
Default Value: 30h Size: 8 bits

Bit	Description
7:0	Serial Bus Release Number (SBRN)— RO. A value of 30h indicates that this controller follows USB release 3.0.

11.2.20 FL_ADJ—Frame Length Adjustment Register (USB xHCI—D20:F0)

Address Offset: 61h
Default Value: 20h
Function Level Reset: No
Attribute: R/W
Size: 8 bits

This feature is used to adjust any offset from the clock source that generates the clock that drives the SOF counter. When a new value is written into these six bits, the length of the frame is adjusted. Its initial programmed value is system dependent based on the accuracy of hardware USB clock and is initialized by system BIOS. This register should only be modified when the HChalted bit (D20:F0:CAPLENGTH + 84h, bit 0) in the USB_STS register is a 1. Changing value of this register while the host controller is operating yields undefined results. It should not be reprogrammed by USB system software unless the default or BIOS programmed values are incorrect, or the system is restoring the register while returning from a suspended state.

These bits in suspend well and not reset by a D3-to-D0 warm rest or a core well reset.

Bit	Description
7:6	Reserved — RO. These bits are reserved for future use and should read as 00b.
5:0	**Frame Length Timing Value** — R/W. Each decimal value change to this register corresponds to 16 high-speed bit times. The SOF cycle time (number of SOF counter clock periods to generate a SOF micro-frame length) is equal to 59488 + value in this field. The default value is decimal 32 (20h), which gives a SOF cycle time of 60000. Frame Length (# 480 MHz Clocks) (decimal) / Frame Length Timing Value (this register) (decimal) 59488 — 0 59504 — 1 59520 — 2 ... — ... 59984 — 31 ... — ... 60496 — 63 60480 — 62 60496 — 63

11.2.21 PWR_CAPID—PCI Power Management Capability ID Register (USB xHCI—D20:F0)

Address Offset: 70h
Default Value: 01h
Attribute: RO
Size: 8 bits

Bit	Description
7:0	**Power Management Capability ID** — RO. A value of 01h indicates that this is a PCI Power Management capabilities field.

11.2.22 NXT_PTR1—Next Item Pointer #1 Register (USB xHCI—D20:F0)

Address Offset: 71h
Default Value: 80h
Attribute: R/W
Size: 8 bits

Bit	Description
7:0	**Next Item Pointer 1 Value** — R/W (special). This register defaults to 80h, which indicates that the next capability registers begin at configuration offset 80h. This register is writable when the ACCTRL bit (D20:F0:40h, bit 31) is '0'. This allows BIOS to effectively hide the next capability registers, if necessary. This register should only be written during system initialization before the plug-and-play software has enabled any master-initiated traffic. Values of 80h implies the next capability is MSI. Values of 00h implies that the MSI capability is hidden.

11.2.23 PWR_CAP—Power Management Capabilities Register (USB xHCI—D20:F0)

Address Offset: 72h–73h
Default Value: C9C2h
Attribute: R/W, RO
Size: 16 bits

Bit	Description
15:11	**PME Support (PME_SUP)** — R/W. This 5-bit field indicates the power states in which the function may assert PME#. Intel® Xeon® Processor D-1500 Product Family xHC does not support the D1 or D2 states. For all other states, Intel® Xeon® Processor D-1500 Product Family xHC is capable of generating PME#. Software should never need to modify this field.
10	D2 Support (D2_SUP) — RO. 0 = D2 State is not supported
9	D1 Support (D1_SUP) — RO. 0 = D1 State is not supported
8:6	**Auxiliary Current (AUX_CUR)** — R/W**.** Intel® Xeon® Processor D-1500 Product Family xHC reports 375 mA maximum suspend well current required when in the $D3_{COLD}$ state.
5	**Device Specific Initialization (DSI**)— RO. Intel® Xeon® Processor D-1500 Product Family reports 0, indicating that no device-specific initialization is required.
4	Reserved
3	**PME Clock (PME_CLK)** — RO. Intel® Xeon® Processor D-1500 Product Family reports 0, indicating that no PCI clock is required to generate PME#.
2:0	**Version (VER)** — RO. Intel® Xeon® Processor D-1500 Product Family reports 010b, indicating that it complies with Revision 1.1 of the PCI Power Management Specification.

Notes:
1. Normally, this register is read-only to report capabilities to the power management software. To report different power management capabilities, depending on the system in which Intel® Xeon® Processor D-1500 Product Family is used, the write access to this register is controlled by the Access Control bit (D20:F0:40h, bit 31). The value written to this register does not affect the hardware other than changing the value returned during a read.
2. This register is modified and maintained by BIOS.
3. Reset: core well, but not D3-to-D0 warm reset.

11.2.24 PWR_CNTL_STS—Power Management Control / Status Register (USB xHCI—D20:F0)

Address Offset: 74h–75h Attribute: R/W, R/WC, RO
Default Value: 0000h Size: 16 bits

Bit	Description
15	**PME Status** — R/WC. This bit is set when Intel® Xeon® Processor D-1500 Product Family xHC would normally assert the PME# signal independent of the state of the PME_En bit. Writing a 1 to this bit will clear it and cause the internal PME to de-assert (if enabled). ***Note:*** This bit must be explicitly cleared by the operating system each time the operating system is loaded. This bit is not reset by Function Level Reset.
14:13	Data Scale — RO. Hardwired to 00b indicating it does not support the associated Data register.
12:9	Data Select — RO. Hardwired to 0000b indicating it does not support the associated Data register.
8	**PME Enable (PME_En)**— R/W. 0 = Disable. 1 = Enables Intel® Xeon® Processor D-1500 Product Family xHC to generate an internal PME signal when PME_Status is 1. ***Note:*** This bit must be explicitly cleared by the operating system each time it is initially loaded. This bit is not reset by Function Level Reset.
7:2	Reserved
1:0	**Power State** — R/W. This 2-bit field is used both to determine the current power state of EHC function and to set a new power state. The definition of the field values are: 00 = D0 state 11 = $D3_{HOT}$ state If software attempts to write a value of 10b or 01b in to this field, the write operation must complete normally; however, the data is discarded and no state change occurs. When in the $D3_{HOT}$ state, Intel® Xeon® Processor D-1500 Product Family must not accept accesses to the EHC memory range; but the configuration space must still be accessible.

11.2.25 MSI_CAPID—Message Signaled Interrupt Capability ID Register (USB xHCI—D20:F0)

Address Offset: 80h Attribute: RO
Default Value: 05h Size: 8 bits

Bit	Description
7:0	**Capability ID** — RO. Hardwired to 05h indicating that this is the start of a MSI Capability structure.

11.2.26 NEXT_PTR2— Next Item Pointer Register #2 (USB xHCI—D20:F0)

Address Offset: 81h Attribute: RO
Default Value: 00h Size: 8 bits
Function Level Reset: No

Bit	Description
7:0	**Next Item Pointer Capability** — RO. This register points to the next capability.

11.2.27 MSI_MCTL— MSI Message Control Register (USB xHCI—D20:F0)

Address Offset: 82h-83h
Attribute: RO, R/W
Default Value: 0086h
Size: 16 bits

Bit	Description
15:8	Reserved.
7	**64 Bit Address Capable (C64)** — RO. Capable of generating 64-bit messages.
6:4	**Multiple Message Enable (MME)** — RW. Indicates the number of messages the controller should assert. This device supports multiple message MSI.
3:1	**Multiple Message Capable (MMC)** — RO. This field is set by HW to reflect the number of Interrupters supported. The controller supports up to 8 interrupters. Encoding for number of Interrupters: 000 1 001 2 010 4 011 8 100 16 101 32 110-111 Reserved
0	**MSI Enable (MSIE)** — RW. If set to 1, MSI is enabled and the traditional interrupt pins are not used to generate interrupts. If cleared to 0, MSI operation is disabled and the traditional interrupt pins are used.

11.2.28 MSI_LMAD—MSI Lower Message Address Register (USB xHCI—D20:F0)

Address Offset: 84h-87h
Attribute: R/W, RO
Default Value: 00000000h
Size: 32 bits

Bit	Description
31:2	**Lower Message Address** — RW. Lower DWord of the system specified message address.
1:0	Reserved.

11.2.29 MSI_UMAD—MSI Upper Message Address Register (USB xHCI—D20:F0)

Address Offset: 88h-8Bh
Attribute: R/W
Default Value: 00000000h
Size: 32 bits

Bit	Description
31:0	**Upper Message Address** — RW. Upper DWord of the system specified message address.

11.2.30 MSI_MD—MSI Message Data Register (USB xHCI—D20:F0)

Address Offset: 8Ch-8Fh
Attribute: R/W
Default Value: 00000000h
Size: 32 bits

Bit	Description
31:16	Reserved.
15:0	**Data** — R/W. This 16-bit field is programmed by system software if MSI is enabled. Its content is driven onto the lower word (PCI AD[15:0]) during the data phase of the MSI memory write transaction.

11.2.31 U2OCM1 - XHCI USB2 Overcurrent Mapping Register1 (USB xHCI—D20:F0)

Address Offset: C0–C3h
Default Value: 00000000h
Attribute: R/W, RO
Size: 32 bits

Bit	Description
31:24	**OC3 Mapping** Each bit position maps OC3# to a set of ports as follows: The OC3# pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 31 30 29 28 27 26 25 24 Port X X X X X X 1 0
23:16	**OC2 Mapping** Each bit position maps OC2# to a set of ports as follows: The OC2# pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 23 22 21 20 19 18 17 16 Port X X X X X X 1 0
15:8	**OC1 Mapping** Each bit position maps OC1# to a set of ports as follows: The OC1# pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 15 14 13 12 11 10 9 8 Port X X X X X X 1 0
7:0	**OC0 Mapping** Each bit position maps OC0# to a set of ports as follows: The OC0# pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 7 6 5 4 3 2 1 0 Port X X X X X X 1 0

11.2.32 U2OCM2 - XHCI USB2 Overcurrent Mapping Register 2 (USB xHCI—D20:F0)

Address Offset: C4–C7h
Default Value: 00000000h
Attribute: R/W, RO
Size: 32 bits

Bit	Description
31:30	Reserved
29:24	**OC7 Mapping** Each bit position maps OC7 to a set of ports as follows: The OC7 pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 29 28 27 26 25 24 Port X X X X 5 4
23:22	Reserved
21:16	**OC6 Mapping** Each bit position maps OC6 to a set of ports as follows: The OC6 pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 21 20 19 18 17 16 Port X X X X 5 4
15:14	Reserved

Bit	Description
13:8	**OC5 Mapping** Each bit position maps OC5 to a set of ports as follows: The OC5 pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 13 12 11 10 9 8 Port X X X X 5 4
7:6	Reserved
5:0	**OC4 Mapping** Each bit position maps OC4 to a set of ports as follows: The OC4 pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 5 4 3 2 1 0 Port X X X X 5 4

11.2.33 U3OCM1 - XHCI USB3 Overcurrent Pin Mapping 1 (USB xHCI—D20:F0)

Address Offset: C8–CBh Attribute: R/W, RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:30	Reserved
29:24	**OC3 Mapping** Each bit position maps OC3to a set of ports as follows: The OC3 pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 29 28 27 26 25 24 Port 6 5 X X 2 1
23:22	Reserved
21:16	**OC2 Mapping** Each bit position maps OC2 to a set of ports as follows: The OC2 pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 21 20 19 18 17 16 Port 6 5 X X 2 1
15:14	Reserved
13:8	**OC1 Mapping** Each bit position maps OC1 to a set of ports as follows: The OC1 pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 13 12 11 10 9 8 Port 6 5 X X 2 1
7:6	Reserved
5:0	**OC0 Mapping** Each bit position maps OC0 to a set of ports as follows: The OC0 pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 5 4 3 2 1 0 Port 6 5 X X 2 1

11.2.34 U3OCM2 - XHCI USB3 Overcurrent Pin Mapping 2 (USB xHCI—D20:F0)

Address Offset: CC–CFh Attribute: R/W, RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:30	Reserved
29:24	**OC7 Mapping** Each bit position maps OC7 to a set of ports as follows: The OC7 pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 29 28 27 26 25 24 Port 6 5 X X 2 1
23:22	Reserved
21:16	**OC6 Mapping** Each bit position maps OC6 to a set of ports as follows: The OC6 pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 21 20 19 18 17 16 Port 6 5 X X 2 1
15:14	Reserved
13:8	**OC5 Mapping** Each bit position maps OC5 to a set of ports as follows: The OC5 pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 13 12 11 10 9 8 Port 6 5 X X 2 1
7:6	Reserved
5:0	**OC4 Mapping** Each bit position maps OC4 to a set of ports as follows: The OC4 pin is ganged to the overcurrent signal of each port that has its corresponding bit set. It is software responsibility to ensure that a given port's bit map is set only for one OC pin. Bit 5 4 3 2 1 0 Port 6 5 X X 2 1

11.2.35 XUSB2PR —xHC USB 2.0 Port Routing Register (USB xHCI—D20:F0)

Address Offset: D0–D3h Attribute: R/W, RO
Default Value: 00000000h Size: 32 bits

Note: Bits 3:0 are located in the Suspend Well.

Bit	Description
31:15	Reserved.
14:0	**USB 2.0 Host Controller Selector (USB2HCSEL)** — R/W. Maps a USB 2.0 port to the xHC or EHC #1 host controller. When cleared to 0, this bit routes all the corresponding USB 2.0 port pins to the EHCI controller (D29:F0) and RMH #1. The USB 2.0 port is masked from the xHC and the USB 2.0 port's OC pin is routed to the EHCI controller (D29:F0). When set to 1, this bit routes all the corresponding USB 2.0 pins to the xHC controller. The USB 2.0 port is masked from the EHC and the USB 2.0 port's OC pin is routed to the xHC controller (D20:F0). Port to bit mapping is in one-hot encoding; that is, bit 0 controls port 1 and so on. Bit 0 = USB 2.0 Port 0 .... Bit 13 = USB 2.0 Port 13

11.2.36 XUSB2PRM—xHC USB 2.0 Port Routing Mask Register (USB xHCI—D20:F0)

Address Offset:	D4–D7h	Attribute:	RO, R/WLO
Default Value:	00000000h	Size:	32 bits

Note: The R/WL property of this register is controlled by the ACCTRL bit (D20:F0:40h, bit 31).

Bit	Description
31:15	Reserved.
14:0	**USB 2.0 Host Controller Selector Mask (USB2HCSELM)** — R/W. This bit field allows the BIOS to communicate to the OS which USB 2.0 ports can be switched from the EHC controller to the xHC controller. When set to 1, the OS may switch the USB 2.0 port between the EHCI and xHCI host controllers by modifying the corresponding USB2HCSEL bit (D20:F0:D0h, bit 3:0). When cleared to 0, The OS shall not modify the corresponding USB2HCSEL bit. Port to bit mapping is in one-hot encoding: that is, bit 0 controls port 1 and so on. Bit 0 = USB 2.0 Port 0 .... Bit 13 = USB 2.0 Port 13

11.2.37 USB3_PSSEN—USB 3.0 Port SuperSpeed Enable Register (USB xHCI—D20:F0)

Address Offset:	D8h–dBh	Attribute:	RO, R/W
Default Value:	00000000h	Size:	32 bits

Note: Bits 3:0 are located in the Suspend Well.

Bit	Description
31:6	Reserved.
5:0	**USB 3.0 Port SuperSpeed Enable (USB3PSSEN)** — R/W. This field controls whether SuperSpeed capability is enabled for a given USB 3.0 port. When set to 1, this bit enables the SuperSpeed terminations and allows the xHC to view the SuperSpeed connections on the USB port. Enables PORTSC to see the connects on the ports. When cleared to 0, the port's SuperSpeed capability is not visible to the xHC. Bit 0 = USB 3.0 Port 1 Bit 1 = USB 3.0 Port 2 Bit 2 = N/A Bit 3 = N/A Bit 4 = USB 3.0 Port 5 Bit 5 = USB 3.0 Port 6

11.2.38 USB3PRM—USB 3.0 Port Routing Mask Register (USB xHCI—D20:F0)

Address Offset:	DC–DFh	Attribute:	RO, R/W
Default Value:	00000000h	Size:	32 bits
Power Well:	Core		

Note: The R/WL property of this register is controlled by the ACCTRL bit (D20:F0:40h, bit 31).

Bit	Description
31:6	Reserved.
5:0	**USB 2.0 Host Controller Selector Mask (USB2HCSELM)** — R/W. This bit field allows the BIOS to communicate to the OS which USB 3.0 ports can have the SuperSpeed capabilities enabled. When set to 1, the OS may enable or disable the SuperSpeed capabilities by modifying the corresponding USB3PSSEN bit (D20:F0:D8h, bit 3:0). When cleared to 0, the OS shall not modify the corresponding USB3PSSEN bit. Bit 0 = USB 3.0 Port 1 Bit 1 = USB 3.0 Port 2 Bit 2 = N/A Bit 3 = N/A Bit 4 = USB 3.0 Port 5 Bit 5 = USB 3.0 Port 6

11.2.39 USB2PDO—xHCI USB Port Disable Override Register (USB xHCI—D20:F0)

Address Offset:	E4–E7h	Attribute:	R/WO
Default Value:	00000000h	Size:	32 bits
Power Well:	Suspend		

Bit	Description
31:15	Reserved.
14:0	**xHCI USB Port Disable Override (XUSBPDO)** — R/WO. 0 = Allows corresponding USB port to report a Device Connection to the xHC. 1 = Prevents the corresponding USB port from reporting a Device Connection to the xHC. Port to bit mapping is in one-hot encoding; that is, bit 0 controls port 1 and so on. Bit 0 = USB 2.0 Port 0 .... Bit 13 = USB 2.0 Port 13

11.2.40 USB3PDO - USB3 Port Disable Override (USB xHCI—D20:F0)

Address Offset:	E8–EBh	Attribute:	R/WO
Default Value:	00000000h	Size:	32 bits
Power Well:	Suspend		

Bit	Description
31:15	Reserved.
14:0	**xHCI USB Port Disable Override (XUSBPDO)** — R/WO. 0 = Allows corresponding USB port to report a Device Connection to the xHC. 1 = Prevents the corresponding USB port from reporting a Device Connection to the xHC. Bit 0 = USB 3.0 Port 1 Bit 1 = USB 3.0 Port 2 Bit 2 = N/A Bit 3 = N/A Bit 4 = USB 3.0 Port 5 Bit 5 = USB 3.0 Port 6

11.3 Memory-Mapped I/O Registers

The xHCI memory-mapped I/O space is composed of two sets of registers: Capability Registers and Operational Registers.

Note: Intel® Xeon® Processor D-1500 Product Family xHC controller will not accept locked memory transactions (neither reads nor writes) as a target. The locked transactions should not be forwarded to PCI as the address space is known to be allocated to USB. Attempting to access the xHCI controller Memory-Mapped I/O space using locked memory transactions will result in undefined behavior.

Note: When the xHCI function is in the D3 PCIe power state, accesses to the xHCI memory range are ignored and result in a master abort. Similarly, if the Memory Space Enable (MSE) bit (D20:F0:04h, bit 1) is not set in the Command register in configuration space, the memory range will not be decoded by Intel® Xeon® Processor D-1500 Product Family xHC. If the MSE bit is not set, Intel® Xeon® Processor D-1500 Product Family must default to allowing any memory accesses for the range specified in the BAR to go to PCI. This is because the range may not be valid and, therefore, the cycle must be made available to any other targets that may be currently using that range.

11.3.1 Host Controller Capability Registers

These registers specify the limits, restrictions and capabilities of the host controller implementation.

Table 11-2. Enhanced Host Controller Capability Registers

MEM_BASE + Offset	Power Well	Mnemonic	Register	Default	Type
00h	Core	CAPLENGTH	Capabilities Registers Length	80h	RW/L
02h–03h	Core	HCIVERSION	Host Controller Interface Version Number	0100h	RO
04h–07h	Core	HCSPARAMS1	Host Controller Structural Parameters #1	15000820h	RW/L
08h–0Bh	Core	HCSPARAMS2	Host Controller Structural Parameters #2	84000054h	RW/L
0Ch–0Fh	Core	HCSPARAMS3	Host Controller Structural Parameters #3	00040001h	RW/L

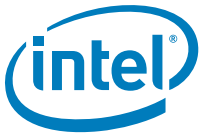


Table 11-2. Enhanced Host Controller Capability Registers

MEM_BASE + Offset	Power Well	Mnemonic	Register	Default	Type
10h–13h	Core	HCCPARAMS	Host Controller Capability Parameters	200071E9h	RW/L
14h–17h	Core	dBOFF	Doorbell Offset	0000C000h	RO
18h–1Bh	Core	RTSOFF	Runtime Register Space Offset	00001000h	RO

11.3.1.1 CAPLENGTH—Capability Registers Length Register

Offset: MEM_BASE + 00h Attribute: RW/L
Default Value: 80h Size: 8 bits

Bit	Description
7:0	**Capability Register Length Value** — RW. This register is used as an offset to add to the Memory Base Register (D20:F0:10h) to find the beginning of the Operational Register Space. This register is modified and maintained by BIOS.

11.3.1.2 HCIVERSION—Host Controller Interface Version Number Register

Offset: MEM_BASE + 02h–03h Attribute: RO
Default Value: 0100h Size: 16 bits

Bit	Description
15:0	**Host Controller Interface Version Number** — RO. This is a two-byte register containing a BCD encoding of the version number of interface that this host controller interface conforms to.

11.3.1.3 HCSPARAMS1—Host Controller Structural Parameters #1 Register

Offset: MEM_BASE + 04h–07h Attribute: RW/L
Default Value: 15000820h Size: 32 bits

Bit	Description
31:24	**Number of Ports (MaxPorts)**— RW/L. This field specifies the number of physical downstream ports implemented on this host controller. The value of this field determines how many port registers are addressable in the Operational Register Space. Default value = 15h
23:19	Reserved
18:8	**Number of Interrupters (MaxIntrs)** — RW/L. This field specifies the number of interrupters implemented on this host controller. Each interrupter is allocated to a vector of MSI and controls its generation and moderation.
7:0	**Number of Device Slots (MaxSlots)** — RW/L. This field specifies the number of Device Context Structures and Doorbell Array entries this host controller can support. Valid values are in the range of 1 to 255.

11.3.1.4 HCSPARAMS2—Host Controller Structural Parameters #2 Register

Offset: MEM_BASE + 08h–0Bh Attribute: RW/L
Default Value: 84000054h Size: 32 bits

Bit	Description
31:27	**Max Scratchpad Buffers (MaxScratchpadBufs)** — RW/L. Indicates the number of Scratchpad Buffers system software shall reserve for the xHC.
26	**Scratchpad Restore (SPR)** — RW/L. 0 = Indicates the Scratchpad buffer space may be freed and reallocated between power events. 1 = Indicates that the xHC requires the integrity of the Scratchpad buffer space to be maintained across power events.
25:8	Reserved.
7:4	**Event Ring Segment Table Max (ERSTMax):** — RW/L. This field determines the maximum value supported by the Event Ring Segment Table Base Size registers.

Bit	Description
3:0	**Isochronous Scheduling Threshold (IST)** — RW/L. This field indicates to system software the minimum distance (in time) that it is required to stay ahead of the xHC while adding TRBs, in order to have the xHC process them at the correct time. The value is specified in the number if frames/ microframes. If bit [3] of IST is cleared o 0b, software can add a TRB no later than IST [2:0] microframes before that TRB is scheduled to be executed. If bit [3] of IST is set to 1b, software can add a TRB no later than IST[2:0] frames before that TRB is scheduled to be executed.

11.3.1.5 HCSPARAMS3—Host Controller Structural Parameters #3 Register

Offset: MEM_BASE + 0Ch–0Fh Attribute: RW/L
Default Value: 00040001h Size: 32 bits

Bit	Description
31:16	**U2 Device Exit Latency (U2DEL)** — RW/L. Indicates the worst case latency to transition from U2 to U0. Applies to all root hub ports. The following are permissible values: **Value** — **Description** 00h — Zero 01h — Less than 1 µs 02h — Less than 2 µs ... 0Bh-FFh — Reserved
15:8	Reserved.
7:0	**U1 Device Exit Latency (U1DEL)** — RW/L. Worst case latency to transition a root hub Port Link State (PLS) from U1 to U0. Applies to all root hub ports. The following are permissible values: **Value** — **Description** 00h — Zero 01h — Less than 1 µs 02h — Less than 2 µs ... 0800h-FFFFh — Reserved

11.3.1.6 HCCPARAMS—Host Controller Capability Parameters Register

Offset: MEM_BASE + 10h–13h Attribute: RW/L
Default Value: 200071E9h Size: 32 bits

Bit	Description
31:16	**xHCI Extended Capabilities Pointer (xECP)** — RW/L This field indicates the existence of a capabilities list. The value of this field indicates a relative offset, in 32-bit words, from Base to the beginning of the first extended capability.
15:12	**Maximum Primary Stream Array Size (MaxPSASize)** — RW/L. This fields identifies the maximum size Primary Stream Array that the xHC supports. The Primary Stream Array size = $2^{MaxPSASize+1}$. Valid MaxPSASize values are 1 to 15.
11	Reserved.
10	**Stopped EDLTA Capability (SEC)** — RW/L. This flag indicates that the host controller implementation Stream Context support a Stopped EDLTA field.
9	**Stopped Short Packet Capability (SPC)** — RW/L. This flag indicates that the host controller implementation is capable of generating a Stopped - Short Packet Completion Code.
8	Reserved.
7	**No Secondary SID Support (NSS)** — RW/L. Hardwired to '0' indicating Secondary Stream ID decoding is supported.

Bit	Description
6	**Latency Tolerance Messaging Capability (LTC)** — RW/L. 0 = Latency Tolerance Messaging is not supported. 1 = Latency Tolerance Messaging is supported
5	**Light HC Reset Capability (LHRC)** — RW/L. 0 = Light Host Controller Reset is not supported. 1 = Light Host Controller Reset is supported
4	**Port Indicators (PIND)** — RW/L. This bit indicates whether the xHC root hub ports support port indicator control. When this bit is a '1', the port status and control registers include a read/writeable field for controlling the state of the port indicator.
3	**Port Power Control (PPC)** — RO. This bit indicates whether the host controller implementation includes port power control. A '1' in this bit indicates the ports have port power switches. A '0' in this bit indicates the port do not have port power switches.
2	**Context Size (CSZ)** — RW/L. If this bit is set to '1', then the xHC uses 64 byte Context data structures. If this bit is cleared to '0', then the xHC uses 32 byte Context data structures. ***Note:*** This flag does not apply to Stream Contexts.
1	**BW Negotiation Capability (BNC)** — RW/L. 0 = Not capable of BW Negotiation. 1 = Capable of BW Negotiation.
0	**64-bit Addressing Capability (AC64)** — RW/L. This bit documents the addressing range capability of the xHC. The value of this flag determines whether the xHC has implemented the high order 32 bits of 64 bit register and data structure pointer fields. Values for this flag have the following interpretation: 0 = Supports 32-bit address memory pointers 1 = Supports 64-bit address memory pointers If 32-bit address memory pointers are implemented, the xHC shall ignore the high order 32 bits of 64 bit data structure pointer fields, and system software shall ignore the high order 32 bits of 64 bit xHC registers.

11.3.1.7 dBOFF—Doorbell Offset Register

Offset:	MEM_BASE + 14h–17h	Attribute:	RO
Default Value:	0000C000h	Size:	32 bits

Bit	Description
31:2	**Doorbell Array Offset** — RO. This field defines the DWord offset of the Doorbell Array base address from the Base (that is, the base address of the xHCI Capability register address space).
1:0	Reserved.

11.3.1.8 RTSOFF—Runtime Register Space Offset Register

Offset:	MEM_BASE + 18h–1Bh	Attribute:	RO
Default Value:	00001000h	Size:	32 bits

Bit	Description
31:2	**Runtime Register Space Offset**— RO. This field defines the 32-byte offset of the xHCI Runtime Registers from the Base. That is, Runtime Register Base Address = Base + Runtime Register Set Offset.
1:0	Reserved.

11.3.2 Host Controller Operational Registers

This section defines the xHC operational registers. These registers are located after the capabilities registers. The operational register base must be DWord-aligned and is calculated by adding the value in the first capabilities register (CAPLENGTH) to the base address of the xHC register address space (MEM_BASE). Since CAPLENGTH is always 80h, Table 11-3 already accounts for this offset. All registers are 32 bits in length.

Table 11-3. Enhanced Host Controller Operational Register Address Map

MEM_BASE + Offset	Power Well	Mnemonic	Register Name	Default	Type
80h–83h	Core	USB_CMD	USB Command	00000000h	R/W, RO
84h–87h	Core	USB_STS	USB Status	00000001h	R/WC, RO
88h–8Bh	Core	PAGESIZE	Page Size	00000001h	RO
94h–97h	Core	DNCTRL	Device Notification Control	00000000h	R/W, RO
98h–9Bh	Core	CRCRL	Command Ring Control Low	00000000h	R/W, RO
9Ch–9Fh	Core	CRCRH	Command Ring Control High	00000000h	R/W, RO
B0h–B3h	Core	DCBAAPL	Device Context Base Address Array Pointer Low	00000000h	R/W, RO
B4h–B7h	Core	DCBAAPH	Device Context Base Address Array Pointer High	00000000h	R/W, RO
B8h–BBh	Core	CONFIG	Configure	00000000h	R/W, RO
480h, 490h, 4A0h, 4B0h, 4C0h, 4D0h, 4E0h, 4F0h, 500h, 510h, 520h, 530h, 540h, 550h, 560h	Multiple	PORTSCNUSB2	Port N Status and Control USB2	000002A0h	R/W, R/WC, RO, R/WO, R/WOC
484h, 494h, 4A4h, 4B4h, 4C4h, 4D4h, 4E4h, 4F4h, 504h, 514h, 524h, 534h, 544h, 554h, 564h	Multiple	PORTPMSCNUSB2	Port N Power Management Status and Control USB2	00000000h	R/W, RO
570h, 580h, 590h, 5A0h, 5B0h, 5C0h	Multiple	PORTSCNUSB3	Port N Status and Control USB3	000002A0h	R/W, RO
574h, 584h, 594h, 5A4h, 5B4h, 5C4h	Suspend	PORTPMSCN	Port N Power Management Status and Control USB3	00000000h	R/W, RO
578h, 588h, 598h, 5A8h, 5B8h, 5C8h	Core	PORTLIX	USB 3.0 Port Link Info	00000000h	RO

Note: Software must read and write these registers using only DWord accesses.

11.3.2.1 USB_CMD—USB Command Register

Offset:	MEM_BASE + 80h–83h	Attribute:	R/W, RO
Default Value:	00000000h	Size:	32 bits

Bit	Description
31:12	Reserved.
11	**Enable U3 MFINDEX Stop (EU3S)** — R/W. When set to 1b, the xHC may stop the MFINDEX counting action if all Root Hub ports are in the U3, Disconnected, Disabled, or Powered-off state. When cleared to 0b, the xHC may stop the MFINDEX counting action if all Root Hub ports are in the Disconnected, Disabled, or Powered-off state.
10	**Enable Wrap Event (EWE)** — R/W. When set to 1b, the xHC shall generate a MFINDEX Wrap Event every time the MFINDEX register transitions from 03FFFh to 0. When cleared to 0b, no MFINDEX Wrap Events are generated.
9	**Controller Restore State (CRS)** — R/W. When set to 1b, MEM_BASE+80h:bit 0= 0b, and MEM_BASE+80h:bit 8 = 1b, the xHC shall perform a Restore State operation and restore its internal state. When set to 1b and MEM_BASE+80h:bit 0= 1b **or** MEM_BASE+80h:bit 8 = 0b, or when cleared to '0', no Restore State operation shall be performed. ***Note:*** This flag always returns '0' when read.
8	**Controller Save State (CSS)** — R/W. When written by software with 1b and MEM_BASE+80h:bit 0= 0b, the xHC shall save any internal state that will be restored by a subsequent Restore State operation. When written by software with 1b and MEM_BASE+80h:bit 0= 1b, or written with '0', no Save State operation shall be performed. ***Note:*** This flag always returns '0' when read.
7	**Light Host Controller Reset (LHCRST)** — R/W. If the Light HC Reset Capability (LHRC) bit (MEM_BASE=10h:bit 5) is 1b, then setting this bit to 1b allows the driver to reset the xHC without affecting the state of the ports. A system software read of this bit as 0b indicates the Light Host Controller Reset has completed and it is safe for software to re-initialize the xHC. A software read of this bit as a 1b indicates the Light Host Controller Reset has not yet completed. ***Note:*** If Light HC Reset Capability is not implemented, a read of this flag will always return a 0b.
6:4	Reserved.
3	**Host System Error Enable (HSEE)** — R/W. When this bit is set to 1b, and the HSE bit (MEM_BASE+84h:bit 2) is set to 1b, the xHC shall assert out-of-band error signaling to the host. The signaling is acknowledged by software clearing the HSE bit.
2	**Interrupter Enable (INTE)** — R/W. This bit provides system software with a means of enabling or disabling the host system interrupts generated by interrupters. When this bit is set to 1b, then Interrupter host system interrupt generation is allowed, such that the xHC shall issue an interrupt at the next interrupt threshold if the host system interrupt mechanism (such that MSI, MSIX, and so on) is enabled. The interrupt is acknowledged by a host system interrupt specific mechanism.
1	**Host Controller Reset (HCRST)** — R/W. This control bit is used by software to reset the host controller. When software sets this bit to 1b, the Host Controller resets its internal pipelines, timers, counters, state machines, and so on to their initial value. Any transaction currently in progress on USB is immediately terminated. A USB reset is not driven on downstream ports. PCI Configuration registers are not affected by this reset. All operational registers, including port registers and port state machines are set to their initial values. ***Notes:*** 1. This bit is cleared to 0b by the Host Controller when the reset process is complete. Software cannot terminate the reset process early by writing a 0b to this bit and shall not write any xHC Operational or Runtime registers while HCRST is set to 1b. 2. Software shall not set this bit to 1b when the HCHalted (HCH) bit (MEM_BASE+84h:bit 0) is cleared to 0b. Attempting to reset an actively running host controller will result in undefined behavior.

Bit	Description
0	**Run/Stop (R/S)** — R/W. When set to 1b, the xHC proceeds with execution of the schedule. The xHC continues execution as long as this bit is set to 1b. When this bit is cleared to 0b, the xHC completes the current and any actively pipelined transactions on the USB and then halts. The xHC shall halt within 16 microframes after software clears the Run/Stop bit. The HCHalted (HCH) bit (MEM_BASE+84h:bit 0) indicates when the xHC has finished its pending pipelined transactions and has entered the stopped state. Software shall not write a '1' to this flag unless the xHC is in the Halted state (that is, HCH in the USBSTS register is '1'); doing so will yield undefined results.

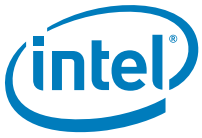
11.3.2.2 USB_STS—USB Status Register

Offset:	MEM_BASE + 84h–87h	Attribute:	R/WC, RO
Default Value:	00000001h	Size:	32 bits

This register indicates pending interrupts and various states of the Host controller. The status resulting from a transaction on the serial bus is not indicated in this register. See the Interrupts description in Section 4 of the xHCI specification for additional information concerning interrupt conditions.

Note: For the writable bits, software must write a 1 to clear bits that are set. Writing a 0 has no effect.

Bit	Description
31:13	Reserved.
12	**Host Controller Error (HCE)** — RO. This flag shall be set to indicate that an internal error condition has been detected which requires software to reset and re-initialize the xHC. 0 = No internal xHC error conditions exist. 1 = Internal xHC error condition exists.
11	**Controller Not Ready (CNR)** — RO. 0 = Ready 1 = Not Ready Software shall not write any Doorbell or Operational register of the xHC, other than the USBSTS register, until CNR = 0b. This flag is set by the xHC after a Hardware Reset and cleared when the xHC is ready to begin accepting register writes. This flag shall remain cleared (0b) until the next Chip Hardware Reset.
10	**Save/Restore Error (SRE)** — R/WC. If an error occurs during a Save or Restore operation this bit shall be set to 1b. This bit shall be cleared to 0b when a Save or Restore operation is initiated or when written with 1b.
9	**Restore State Status (RSS)** — RO. When the Controller Restore State (CRS) flag in the USB_CMD register is written with 1b this bit shall be set to 1b and remain set while the xHC restores its internal state. ***Note:*** When the Restore State operation is complete, this bit shall be cleared to 0b.
8	**Save State Status (SSS)** — RO. When the Controller Save State (CSS) flag in the USB_CMD register is written with 1b this bit shall be set to 1b and remain set while the xHC saves its internal state. ***Note:*** When the Save State operation is complete, this bit shall be cleared to 0b.
7:5	Reserved.
4	**Port Change Detect (PCD)** — R/WC. This bit is allowed to be maintained in the Auxiliary power well. Alternatively, it is also acceptable that on a D3 to D0 transition of the xHC, this bit is loaded with the OR of all of the PORTSC change bits (including: Force port resume, overcurrent change, enable/disable change and connect status change). Regardless of the implementation, when this bit is readable (that is, in the D0 state), it must provide a valid view of the Port Status registers. 0 = No change bit transition from a 0 to 1 or No Force Port Resume bit transition from 0 to 1 as a result of a J-K transition detected on a suspended port. 1 = The Host controller sets this bit to 1 when any port for which the *Port Owner* bit is cleared to 0 has a change bit transition from a 0 to 1 or a Force Port Resume bit transition from 0 to 1 as a result of a J-K transition detected on a suspended port.
3	**Event Interrupt (EINT)** — R/WC. The xHC sets this bit to 1b when the Interrupt Pending (IP) bit of any Interrupter is transitions from 0b to 1b. Software that uses EINT shall clear it prior to clearing any IP flags. A race condition will occur if software clears the IP flags then clears the EINT flag, and between the operations another IP '0' to '1' transition occurs. In this case the new IP transition will be lost.



Bit	Description
2	**Host System Error (HSE)**— R/WC. The xHC sets this bit to 1b when a serious error is detected, either internal to the xHC or during a host system access involving the xHC module. Conditions that set this bit to '1' include PCI Parity error, PCI Master Abort, and PCI Target Abort. When this error occurs, the xHC clears the Run/Stop (R/S) bit in the USB_CMD register to prevent further execution of the scheduled TDs. If the HSEE bit in the USB_CMD register is 1b, the xHC shall also assert out-of-band error signaling to the host.
1	Reserved.
0	**HCHalted (HCH)** — RO. This bit is a '0' whenever the Run/Stop (R/S) bit is set to 1b. The xHC sets this bit to 1b after it has stopped executing as a result of the Run/Stop (R/S) bit being cleared to 0b, either by software or by the xHC hardware (such as internal error). If this bit is set to1b, then SOFs, microSOFs, or Isochronous Timestamp Packets (ITP) shall not be generated by the xHC.

11.3.2.3 PAGESIZE—Page Size Register

Offset:	MEM_BASE + 88h–8Bh	Attribute:	RO
Default Value:	00000001h	Size:	32 bits

Bit	Description
31:16	Reserved
15:0	**Page Size** — RO. Hardwired to 1h to indicate support for 4k byte page sizes.

11.3.2.4 DNCTRL—Device Notification Control Register

Offset:	MEM_BASE + 94h–97h	Attribute:	R/W, RO
Default Value:	00000000h	Size:	32 bits

Bit	Description
31:16	Reserved.
15:0	**Notification Enable** — R/W. When a Notification Enable bit is set, a Device Notification Event will be generated when a Device Notification Transaction Packet is received with the matching value in the Notification Type field. For example, setting N1 to '1' enables Device Notification Event generation if a Device Notification TP is received with its Notification Type field set to '1' (FUNCTION_WAKE), and so on. Refer to the USB 3.0 Specification for more information on Notification Types.

11.3.2.5 CRCRL—Command Ring Control Low Register

Offset:	MEM_BASE + 98h–9Bh	Attribute:	R/W, RO
Default Value:	00000000h	Size:	32 bits

Bit	Description
31:6	**Command Ring Pointer** — R/W. This field defines low order bits of the initial value of the 64-bit Command Ring Dequeue Pointer. ***Notes:*** 1. Writes to this field are ignored when Command Ring Running bit (CRR) = 1b. 2. If the CRCR register is written while the Command Ring is stopped (CRR = 0b), the value of this field shall be used to fetch the first Command TRB the next time the Host Controller Doorbell register is written with the dB Reason field set to Host Controller Command. 3. If the CRCR register is not written while the Command Ring is stopped (CRR = 0b), then the Command Ring shall begin fetching Command TRBs at the current value of the internal xHC Command Ring Dequeue Pointer. 4. Reading this field always returns 0b.
5:4	Reserved.
3	**Command Ring Running (CRR)** — RO. This bit is set to 1b if the Run/Stop (R/S) bit is 1b and the Host Controller Doorbell register is written with the dB Reason field set to Host Controller Command. It is cleared to 0b when the Command Ring is stopped after writing a 1b to the Command Stop (CS) or Command Abort (CA) bits, or if the R/S bit is cleared to 0b.

Bit	Description
2	**Command Abort (CA)** — R/W. Writing a 1b to this bit shall immediately terminate the currently executing command, stop the Command Ring, and generate a Command Completion Event with the Completion Code set to Command Ring Stopped. The next write to the Host Controller Doorbell with dB Reason field set to Host Controller Command shall restart the Command Ring operation. ***Notes:*** 1. Writes to this flag are ignored by the xHC if Command Ring Running (CRR) = 0b. 2. Reading this bit always returns 0b.
1	**Command Stop (CS)** — R/W. Writing a 1b to this bit shall stop the operation of the Command Ring after the completion of the currently executing command, and generate a Command Completion Event with the Completion Code set to Command Ring Stopped and the Command TRB Pointer set to the current value of the Command Ring Dequeue Pointer. The next write to the Host Controller Doorbell with dB Reason field set to Host Controller Command shall restart the Command Ring operation. ***Notes:*** 1. Writes to this flag are ignored by the xHC if Command Ring Running (CRR) bit = 0b. 2. Reading this bit always returns 0b.
0	**Ring Cycle State (RCS)** — R/W. This bit identifies the value of the xHC Consumer Cycle State (CCS) flag for the TRB referenced by the Command Ring Pointer. ***Notes:*** 1. Writes to this bit are ignored when the Command Ring Running (CRR) bit = 1b. 2. If the CRCR register is written while the Command Ring is stopped (CCR = 0b), then the value of this flag shall be used to fetch the first Command TRB the next time the Host Controller Doorbell register is written with the dB Reason field set to Host Controller Command. 3. If the CRCR register is not written while the Command Ring is stopped (CCR = 0b), then the Command Ring will begin fetching Command TRBs using the current value of the internal Command Ring CCS flag. 4. Reading this flag always returns 0b.

Notes:
1. Setting the Command Stop (CS) or Command Abort (CA) flags while CRR = 1b shall generate a Command Ring Stopped Command Completion Event.
2. Setting both the Command Stop (CS) and Command Abort (CA) flags with a single write to the CRCR register while CRR = '1' shall be interpreted as a Command Abort (CA) by the xHC.
3. The values of the internal xHC Command Ring CCS flag and Dequeue Pointer are undefined after hardware reset, so these fields shall be initialized before setting USB_CMD Run/Stop (R/S) bit (MEM_BASE+80:bit 0) to 1b.

11.3.2.6 CRCRH—Command Ring Control High Register

Offset:	MEM_BASE + 9Ch–9Fh	Attribute:	R/W, RO
Default Value:	00000000h	Size:	32 bits

Bit	Description
31:0	**Command Ring Pointer** — R/W. This field defines high order bits of the initial value of the 64-bit Command Ring Dequeue Pointer. ***Notes:*** 1. Writes to this field are ignored when Command Ring Running bit (CRR) = 1b. 2. If the CRCR register is written while the Command Ring is stopped (CRR = 0b), the value of this field shall be used to fetch the first Command TRB the next time the Host Controller Doorbell register is written with the dB Reason field set to Host Controller Command. 3. If the CRCR register is not written while the Command Ring is stopped (CRR = 0b), then the Command Ring shall begin fetching Command TRBs at the current value of the internal xHC Command Ring Dequeue Pointer. 4. Reading this field always returns 0b.

11.3.2.7 DCBAAPL—Device Context Base Address Array Pointer Low Register

Offset: MEM_BASE + B0h–B3h Attribute: R/W, RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:6	**Device Context Base Address Array Pointer** — R/W. This field defines low order bits of the 64-bit base address of the Device Context Pointer Array table (a table of address pointers that reference Device Context structures for the devices attached to the host.)
5:0	Reserved.

11.3.2.8 DCBAAPH—Device Context Base Address Array Pointer High Register

Offset: MEM_BASE + B4h–B7h Attribute: R/W, RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:0	**Device Context Base Address Array Pointer** — R/W. This field defines high order bits of the 64-bit base address of the Device Context Pointer Array table (a table of address pointers that reference Device Context structures for the devices attached to the host.)

11.3.2.9 CONFIG—Configure Register

Offset: MEM_BASE + B8h–BBh Attribute: R/W, RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:8	Reserved.
7:0	**Max Device Slots Enabled (MaxSlotsEn)** — R/W. This field specifies the maximum number of enabled Device Slots. Valid values are in the range of 0h to 20h. Enabled Devices Slots are allocated contiguously (such that a value of 16 specifies that Device Slots 1 to 16 are active.) A value of '0' disables all Device Slots. A disabled Device Slot shall not respond to Doorbell Register references. ***Note:*** This field shall not be modified if the xHC is running (Run/Stop (R/S) = '1').

11.3.2.10 PORTSCNUSB2—Port N Status and Control USB2 Register

Offset: There are 15 USB2 PORTSC registers at offsets:
480h, 490h, 4A0h, 4B0h, 4C0h, 4D0h, 4E0h, 4F0h,
500h, 510h, 520h, 530h, 540h, 550h, 560h

Attribute: R/W, R/WC, RO, R/WO, R/WOC
Default Value: 000002A0h Size: 32 bits

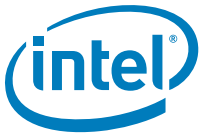
A host controller must implement one or more port registers. Software uses the N_Port information from the Structural Parameters Register to determine how many ports need to be serviced. All ports have the structure defined below. Software must not write to unreported Port Status and Control Registers.

This register is in the suspend power well. It is only reset by hardware when the suspend power is initially applied or in response to a host controller reset. The initial conditions of a port are:

- No device connected
- Port disabled.

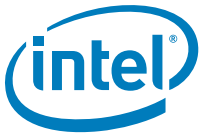
When a device is attached, the port state transitions to the attached state and system software will process this as with any status change notification. See Section 4 of the xHCI Specification for operational requirements for how change events interact with port suspend mode.

Bit	Description
31	**Warm Port Reset (WPR)** — R/WO. When software sets this bit to 1b, the Warm Reset sequence is initiated and the PR bit is set to 1b. Once initiated, the PR, PRC, and WRC bits shall reflect the progress of the Warm Reset sequence. This flag shall always return 0b when read. ***Note:*** This bit applies only to USB 3.0 capable ports. For ports that are only USB 2.0 capable, this bit is Reserved. ***Note:*** This bit is in the Suspend Well.
30	**Device Removable (DR)** — RO. This bit indicates if this port has a removable device attached. 0 = Device is removable. 1 = Device is non-removable. ***Note:*** This bit is in the Core Well.
29:28	Reserved.
27	**Wake on Over-current Enable (WOE)** — R/W. 0 = Disable. (Default) 1 = Enable. Writing this bit to a 1b enables the port to be sensitive to over-current conditions as system wake-up events. ***Note:*** This bit is in the Suspend Well.
26	**Wake on Disconnect Enable (WDE)** — R/W. 0 = Disable. (Default) 1 = Enable. Writing this bit to a 1b enables the port to be sensitive to device disconnects as system wake-up events. ***Note:*** This bit is in the Suspend Well.
25	**Wake on Connect Enable (WCE)** — R/W. 0 = Disable. (Default) 1 = Enable. Writing this bit to a 1b enables the port to be sensitive to device connects as system wake-up events. ***Note:*** This bit is in the Suspend Well.
24	**Cold Attach Status (CAS)** — RO. This bit indicates that far-end terminations were detected in the Disconnected state and the Root Hub Port State Machine was unable to advance to the Enabled state. Software shall clear this bit by writing a 1b to the WPR bit or the xHC shall clear this bit if the CSS bit transitions to 1. ***Note:*** This bit is 0b if the PP bit is 0b or for USB 2.0 capable-only ports. ***Note:*** This bit is in the Suspend Well.
23	**Port Config Error Change (CEC)** — R/WOC. This flag indicates that the port failed to configure its link partner. Software shall clear this bit by writing a 1 to it. ***Note:*** This bit applies only to USB 3.0 capable ports. This bit is Reserved for USB 2.0 capable-only ports. ***Note:*** This bit is in the Suspend Well.



Bit	Description
22	**Port Link State Change (PLC)** — R/WC. 0 = No change 1 = Link Status Change This flag is set to '1' due to the following Port Link State (PLS) transitions: **Transition** / **Condition** U3 -> Resume — Wakeup signaling from a device Resume -> Recovery -> U0 — Device Resume complete (USB 3.0 capable ports only) Resume -> U0 — Device Resume complete (USB 2.0 capable-only ports) U3 -> Recovery -> U0 — Software Resume complete (USB 3.0 capable ports only) U3 -> U0 — Software Resume complete (USB 2.0 capable-only ports) U2 -> U0 — L1 Resume complete (USB 2.0 capable-only ports) U0 -> U0 — L1 Entry Reject (USB 2.0 capable-only ports) U0 -> Disabled — L1 Entry Error (USB 2.0 capable-only ports) Any state -> Inactive — Error (USB 3.0 capable ports only) ***Notes:*** 1. This bit shall not be set if the PLS transition was due to software setting the PP bit to 0b. 2. Software shall clear this bit by writing a 1 to it. 3. This bit is in the Suspend Well.
21	**Port Reset Change (PRC)** — R/WC. This flag is set to '1' due a '1' to '0' transition of Port Reset (PR); such as when any reset processing on this port is complete. 0 = No change 1 = Reset Complete ***Notes:*** 1. This bit shall not be set to 1b if the reset processing was forced to terminate due to software clearing the PP bit or PED bit to 0b. 2. Software shall clear this bit by writing a 1 to it. 3. This bit is in the Suspend Well.
20	**Over-current Change (OCC)** — R/WC. The functionality of this bit is not dependent upon the port owner. Software clears this bit by writing a 1 to it. 0 = No change. (Default) 1 = There is a change to Overcurrent Active. ***Note:*** This bit is in the Suspend Well.
19	**Warm Port Reset Change (WRC)** — R/WC. This bit is set when Warm Reset processing on this port completes. 0 = No change. (Default) 1 = Warm reset complete ***Notes:*** 1. This bit shall not be set to 1b if the reset processing was forced to terminate due to software clearing the PP bit or PED bit to 0b. 2. Software shall clear this bit by writing a 1 to it. 3. This bit applies only to USB 3.0 capable ports. This bit is Reserved for USB 2.0 capable-only ports. 4. This bit is in the Suspend Well.
18	**Port Enabled/Disabled Change (PEC)** — R/WC. 0 = No change. (Default) 1 = There is a change to PED bit. ***Notes:*** 1. This bit shall not be set if the PED transition was due to software setting the PP bit to 0. 2. Software shall clear this bit by writing a 1 to it. 3. For a USB 2.0-only port, this bit shall be set to 1 only when the port is disabled due to the appropriate conditions existing at the EOF2 point. (See Chapter 11 of the USB Specification for the definition of a port error). 4. For a USB 3.0 port, this bit shall be set to '1' if an enabled port transitions to a Disabled state (that is, a '1' to '0' transition of PED). Refer to Section 4 of the xHCI Specification for more information. 5. This bit is in the Suspend Well.

Bit	Description
17	**Connect Status Change (CSC)** — R/WC. This flag indicates a change has occurred in the port's Current Connect Status (CCS) or Cold Attach Status (CAS) bits. 0 = No change. (Default) 1 = There is a change to the CCS or CAS bit. The xHC sets this bit to 1b for all changes to the port device connect status, even if system software has not cleared an existing Connect Status Change. For example, the insertion status changes twice before system software has cleared the changed condition, root hub hardware will be "setting" an already-set bit (that is, the bit will remain 1b). ***Notes:*** 1. This bit shall not be set if the CCS transition was due to software setting the PP bit to 0b, or the CAS bit transition was die to software setting the WPR bit to 1b. 2. Software shall clear this bit by writing a 1 to it. 3. This bit is in the Suspend Well.
16	**Port Link State Write Strobe (LWS)** — R/W. 0 = When 0b, write data in PLS field is ignored. (Default) 1 = When this bit is set to 1b on a write reference to this register, this flag enables writes to the PLS field. Reads to this bit return '0'. ***Note:*** This bit is in the Suspend Well.
15:14	Reserved.
13:10	**Port Speed (Port_Speed).** A device attached to this port operates at a speed defined by the following codes: Value — Speed 0001b — Full-speed (12 Mb/s) 0010b — Low-speed (1.5 Mb/s) 0011b — High-speed (480 Mb/s) All other values reserved. Refer to the eXtensible Host Controller Interface for Universal Serial Bus Specification for additional details. ***Note:*** This bit is in the Suspend Well.
9	**Port Power (PP)** — RO. Read-only with a value of 1. This indicates that the port does have power. ***Note:*** This bit is in the Suspend Well.



<table>
<tr><th>Bit</th><th>Description</th></tr>
<tr><td>8:5</td><td>
Port Link State (PLS) — R/W. This field is used to power manage the port and reflects its current link state.
When the port is in the Enabled state, system software may set the link U-state by writing this field. System software may also write this field to force a Disabled to Disconnected state transition of the port.
<table>
<tr><th>Write Value</th><th>Description</th></tr>
<tr><td>0</td><td>The link shall transition to a U0 state from any of the U-states.</td></tr>
<tr><td>2</td><td>USB 2.0 ports only. The link should transition to the U2 State.</td></tr>
<tr><td>3</td><td>The link shall transition to a U3 state from any of the U-states. This action selectively suspends the device connected to this port. While the Port Link State = U3, the hub does not propagate downstream-directed traffic to this port, but the hub will respond to resume signaling from the port.</td></tr>
<tr><td>5</td><td>USB 3.0 ports only. If the port is in the Disabled state (PLS = Disabled, PP = 1), then the link shall transition to a RxDetect state and the port shall transition to the Disconnected state, else ignored.</td></tr>
<tr><td>15</td><td>USB 2.0 ports only. If the port is in the U3 state (PLS = U3), then the link shall remain in the U3 state and the port shall transition to the U3Exit substate, else ignored.</td></tr>
<tr><td>All other values</td><td>Ignored</td></tr>
</table>
Note: The Port Link State Write Strobe (LWS) shall be set to 1b to write this field.
<table>
<tr><th>Read Value</th><th>Definition</th></tr>
<tr><td>0</td><td>Link is in the U0 State</td></tr>
<tr><td>1</td><td>Link is in the U1 State</td></tr>
<tr><td>2</td><td>Link is in the U2 State</td></tr>
<tr><td>3</td><td>Link is in the U3 State (Device Suspended)</td></tr>
<tr><td>4</td><td>Link is in the Disabled State</td></tr>
<tr><td>5</td><td>Link is in the RxDetect State</td></tr>
<tr><td>6</td><td>Link is in the Inactive State</td></tr>
<tr><td>7</td><td>Link is in the Polling State</td></tr>
<tr><td>8</td><td>Link is in the Recovery State</td></tr>
<tr><td>9</td><td>Link is in the Hot Reset State</td></tr>
<tr><td>10</td><td>Link is in the Compliance Mode State</td></tr>
<tr><td>11</td><td>Link is in the Test Mode State</td></tr>
<tr><td>12-14</td><td>Reserved</td></tr>
<tr><td>15</td><td>Link is in the Resume State</td></tr>
</table>
Notes:
1. This field is undefined if PP = 0.
2. Transitions between different states are not reflected until the transition is complete.
3. This bit is in the Suspend Well.
</td></tr>
<tr><td>4</td><td>
Port Reset (PR) — R/W. When software writes a 1 to this bit (from a 0), the bus reset sequence as defined in the USB Specification, Revision 2.0 is started. Software writes a 0 to this bit to terminate the bus reset sequence. Software must keep this bit at a 1 long enough to ensure the reset sequence completes as specified in the USB Specification, Revision 2.0. USB 3.0 ports shall execute the Hot Reset sequence as defined in the USB 3.0 Specification. PR remains set until reset signaling is completed by the root hub.
1 = Port is in Reset.
0 = Port is not in Reset.
Note: This bit is in the Suspend Well.
</td></tr>
<tr><td>3</td><td>
Overcurrent Active (OCA)— RO.
0 = This port does not have an overcurrent condition. (Default)
1 = This port currently has an overcurrent condition. This bit will automatically transition from 1 to 0 when the over current condition is removed. Intel® Xeon® Processor D-1500 Product Family automatically disables the port when the overcurrent active bit is 1.
Note: This bit is in the Suspend Well.
</td></tr>
</table>

Bit	Description
2	Reserved.
1	**Port Enabled/Disabled** — R/W. Ports can only be enabled by the host controller as a part of the reset and enable. Software cannot enable a port by writing a 1 to this bit. Ports can be disabled by either a fault condition (disconnect event or other fault condition) or by host software. The bit status does not change until the port state actually changes. There may be a delay in disabling or enabling a port due to other host controller and bus events. 0 = Disable 1 = Enable (Default) ***Note:*** This bit is in the Suspend Well.
0	**Current Connect Status** — RO. This value reflects the current state of the port, and may not correspond directly to the event that caused the Connect Status Change bit (Bit 1) to be set. 0 = No device is present. (Default) 1 = Device is present on port. ***Note:*** This bit is in the Suspend Well.

11.3.2.11 PORTPMSCNUSB2—xHCI Port N Power Management Status and Control USB2 Register

Offset: There are 15 USB2 PORTPMSC registers at offsets: 484h, 494h, 4A4h, 4B4h, 4C4h, 4D4h, 4E4h, 4F4h, 504h, 514h, 524h, 534h, 544h, 554h, 564h

Attribute: R/W, RO

Default Value: 00000000h Size: 32 bits

Bit	Description
31:28	**Port Test Control** — R/W. When this field is '0', the port is not operating in a test mode. (Default) A non-zero value indicates that the port is operating in test mode and the specific test mode is indicated by the specific value. A non-zero Port Test Control value is only valid to a port that is in the Disabled state. If the port is not in this state, the xHC shall respond with the Port Test Control field set to Port Test Control Error. The encoding of the Test Mode bits for a USB 2.0 port are: **Value** — **Test Mode** 0h — Test mode not enabled 1h — Test J_STATE 2h — Test K_STATE 3h — Test SE0_NAK 4h — Test Packet 5h — Test FORCE_ENABLE 6h-14h — Reserved. 15 — Port Test Control Error See Sections 7.1.20 and 11.24.2.13 of the USB 2.0 Specification for more information on Test Modes. ***Note:*** This bit is in the Suspend Well.
27:17	Reserved.
16	**Hardware LPM Enable (HLE)** — RO. 0 = Disable. 1 = Enable. When this bit is a 1, hardware controlled LPM shall be enabled for this port. See Section 4 of the USB 2.0 LPM Specification for more information. ***Note:*** This bit is in the Suspend Well.
15:8	**L1 Device Slot** — R/W. System software sets this field to indicate the ID of the Device Slot associated with the device directly attached to the Root Hub port. A value of 0 indicates there is no device present. ***Note:*** This bit is in the Suspend Well.

Bit	Description
7:4	**Host Initiated Resume Duration (HIRD)** — R/W. System software sets this field to indicate to the recipient device how long the xHC will drive resume if it (the xHC) initiates an exit from L1. The HIRD value is encoded as follows: The value of 0000b is interpreted as 50 µs. Each incrementing value up adds 75 µs to the previous value. For example, 0001b is 125 µs, 0010b is 200 µs and so on. Based on this rule, the maximum value resume drive time is at encoding value 1111b which represents 1.2ms. Refer to Section 4 of the USB 2.0 LPM Specification for more information. ***Note:*** This bit is in the Suspend Well.
3	**Remote Wake Enable (RWE)** — R/W. The host system sets this flag to enable or disable the device for remote wake from L1. 0 = Disable. (Default) 1 = Enable. The value of this flag will temporarily (while in L1) override the current setting of the Remote Wake feature set by the standard Set/ClearFeature() commands defined in Universal Serial Bus Specification, revision 2.0, Chapter 9. ***Note:*** This bit is in the Suspend Well.
2:0	**L1 status** - RO. ***Note:*** This bit is in the Suspend Well.

11.3.2.12 PORTSCNUSB3—xHCI USB 3.0 Port N Status and Control Register

Offset: There are 6 USB3 PORTSC registers at offsets: 570h, 580h, 590h, 5A0h, 5B0h, 5C0h
Attribute: R/W,RO
Default Value: 000002A0h Size: 32 bits

A host controller must implement one or more port registers. Software uses the N_Port information from the Structural Parameters Register to determine how many ports need to be serviced. All ports have the structure defined below. Software must not write to unreported Port Status and Control Registers.

This register is in the suspend power well. It is only reset by hardware when the suspend power is initially applied or in response to a host controller reset. The initial conditions of a port are:

- No device connected
- Port disabled.

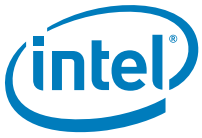
When a device is attached, the port state transitions to the attached state and system software will process this as with any status change notification. See Section 4 of the xHCI Specification for operational requirements for how change events interact with port suspend mode.

Bit	Description
31	**Warm Port Reset (WPR)** — R/WO. When software sets this bit to 1b, the Warm Reset sequence is initiated and the PR bit is set to 1b. Once initiated, the PR, PRC, and WRC bits shall reflect the progress of the Warm Reset sequence. This flag shall always return 0b when read. ***Note:*** This bit applies only to USB 3.0 capable ports. For ports that are only USB 2.0 capable, this bit is Reserved. ***Note:*** This bit is in the Suspend Well.
30	**Device Removable (DR)** — RO. This bit indicates if this port has a removable device attached. 0 = Device is removable. 1 = Device is non-removable. ***Note:*** This bit is in the Core Well.
29:28	Reserved.

Bit	Description
27	**Wake on Over-current Enable (WOE)** — R/W. 0 = Disable. (Default) 1 = Enable. Writing this bit to a 1b enables the port to be sensitive to over-current conditions as system wake-up events. ***Note:*** This bit is in the Suspend Well.
26	**Wake on Disconnect Enable (WDE)** — R/W. 0 = Disable. (Default) 1 = Enable. Writing this bit to a 1b enables the port to be sensitive to device disconnects as system wake-up events. ***Note:*** This bit is in the Suspend Well.
25	**Wake on Connect Enable (WCE)** — R/W. 0 = Disable. (Default) 1 = Enable. Writing this bit to a 1b enables the port to be sensitive to device connects as system wake-up events. ***Note:*** This bit is in the Suspend Well.
24	**Cold Attach Status (CAS)** — RO. This bit indicates that far-end terminations were detected in the Disconnected state and the Root Hub Port State Machine was unable to advance to the Enabled state. Software shall clear this bit by writing a 1b to the WPR bit or the xHC shall clear this bit if the CSS bit transitions to 1. ***Note:*** This bit is 0b if the PP bit is 0b or for USB 2.0 capable-only ports. ***Note:*** This bit is in the Suspend Well.
23	**Port Config Error Change (CEC)** — R/WOC. This flag indicates that the port failed to configure its link partner. Software shall clear this bit by writing a 1 to it. ***Note:*** This bit applies only to USB 3.0 capable ports. This bit is Reserved for USB 2.0 capable-only ports. ***Note:*** This bit is in the Suspend Well.
22	**Port Link State Change (PLC)** — R/WC. 0 = No change 1 = Link Status Change This flag is set to '1' due to the following Port Link State (PLS) transitions: **Transition** — **Condition** U3 -> Resume — Wakeup signaling from a device Resume -> Recovery -> U0 — Device Resume complete (USB 3.0 capable ports only) Resume -> U0 — Device Resume complete (USB 2.0 capable-only ports) U3 -> Recovery -> U0 — Software Resume complete (USB 3.0 capable ports only) U3 -> U0 — Software Resume complete (USB 2.0 capable-only ports) U2 -> U0 — L1 Resume complete (USB 2.0 capable-only ports) U0 -> U0 — L1 Entry Reject (USB 2.0 capable-only ports) U0 -> Disabled — L1 Entry Error (USB 2.0 capable-only ports) Any state -> Inactive — Error (USB 3.0 capable ports only) ***Notes:*** 1. This bit shall not be set if the PLS transition was due to software setting the PP bit to 0b. 2. Software shall clear this bit by writing a 1 to it. 3. This bit is in the Suspend Well.
21	**Port Reset Change (PRC)** — R/WC. This flag is set to '1' due a '1' to '0' transition of Port Reset (PR); such as when any reset processing on this port is complete. 0 = No change 1 = Reset Complete ***Notes:*** 1. This bit shall not be set to 1b if the reset processing was forced to terminate due to software clearing the PP bit or PED bit to 0b. 2. Software shall clear this bit by writing a 1 to it. 3. This bit is in the Suspend Well.

Bit	Description
20	**Over-current Change (OCC)** — R/WC. The functionality of this bit is not dependent upon the port owner. Software clears this bit by writing a 1 to it. 0 = No change. (Default) 1 = There is a change to Overcurrent Active. ***Note:*** This bit is in the Suspend Well.
19	**Warm Port Reset Change (WRC)** — R/WC. This bit is set when Warm Reset processing on this port completes. 0 = No change. (Default) 1 = Warm reset complete ***Notes:*** 1. This bit shall not be set to 1b if the reset processing was forced to terminate due to software clearing the PP bit or PED bit to 0b. 2. Software shall clear this bit by writing a 1 to it. 3. This bit applies only to USB 3.0 capable ports. This bit is Reserved for USB 2.0 capable-only ports. 4. This bit is in the Suspend Well.
18	**Port Enabled/Disabled Change (PEC)** — R/WC. 0 = No change. (Default) 1 = There is a change to PED bit. ***Notes:*** 1. This bit shall not be set if the PED transition was due to software setting the PP bit to 0. 2. Software shall clear this bit by writing a 1 to it. 3. For a USB 2.0-only port, this bit shall be set to 1 only when the port is disabled due to the appropriate conditions existing at the EOF2 point. (See Chapter 11 of the USB Specification for the definition of a port error). 4. For a USB 3.0 port, this bit shall be set to '1' if an enabled port transitions to a Disabled state (that is, a '1' to '0' transition of PED). Refer to Section 4 of the xHCI Specification for more information. 5. This bit is in the Suspend Well.
17	**Connect Status Change (CSC)** — R/WC. This flag indicates a change has occurred in the port's Current Connect Status (CCS) or Cold Attach Status (CAS) bits. 0 = No change. (Default) 1 = There is a change to the CCS or CAS bit. The xHC sets this bit to 1b for all changes to the port device connect status, even if system software has not cleared an existing Connect Status Change. For example, the insertion status changes twice before system software has cleared the changed condition, root hub hardware will be "setting" an already-set bit (that is, the bit will remain 1b). ***Notes:*** 1. This bit shall not be set if the CCS transition was due to software setting the PP bit to 0b, or the CAS bit transition was die to software setting the WPR bit to 1b. 2. Software shall clear this bit by writing a 1 to it. 3. This bit is in the Suspend Well.
16	**Port Link State Write Strobe (LWS)** — R/W. 0 = When 0b, write data in PLS field is ignored. (Default) 1 = When this bit is set to 1b on a write reference to this register, this flag enables writes to the PLS field. Reads to this bit return '0'. ***Note:*** This bit is in the Suspend Well.
15:14	Reserved.
13:10	**Port Speed (Port_Speed).** A device attached to this port operates at a speed defined by the following codes: Value — Speed 0100 — SuperSpeed (5 Gb/s) All other values reserved. Refer to the eXtensible Host Controller Interface for Universal Serial Bus Specification for additional details.
9	**Port Power (PP)** — RO. Read-only with a value of 1. This indicates that the port does have power. ***Note:*** This bit is in the Suspend Well.

<table>
<tr><th>Bit</th><th>Description</th></tr>
<tr><td>8:5</td><td>
Port Link State (PLS) — R/W. This field is used to power manage the port and reflects its current link state.
When the port is in the Enabled state, system software may set the link U-state by writing this field. System software may also write this field to force a Disabled to Disconnected state transition of the port.
<table>
<tr><th>Write Value</th><th>Description</th></tr>
<tr><td>0</td><td>The link shall transition to a U0 state from any of the U-states.</td></tr>
<tr><td>2</td><td>USB 2.0 ports only. The link should transition to the U2 State.</td></tr>
<tr><td>3</td><td>The link shall transition to a U3 state from any of the U-states. This action selectively suspends the device connected to this port. While the Port Link State = U3, the hub does not propagate downstream-directed traffic to this port, but the hub will respond to resume signaling from the port.</td></tr>
<tr><td>5</td><td>USB 3.0 ports only. If the port is in the Disabled state (PLS = Disabled, PP = 1), then the link shall transition to a RxDetect state and the port shall transition to the Disconnected state, else ignored.</td></tr>
<tr><td>15</td><td>USB 2.0 ports only. If the port is in the U3 state (PLS = U3), then the link shall remain in the U3 state and the port shall transition to the U3Exit substate, else ignored.</td></tr>
<tr><td>All other values</td><td>Ignored</td></tr>
</table>
Note: The Port Link State Write Strobe (LWS) shall be set to 1b to write this field.
<table>
<tr><th>Read Value</th><th>Definition</th></tr>
<tr><td>0</td><td>Link is in the U0 State</td></tr>
<tr><td>1</td><td>Link is in the U1 State</td></tr>
<tr><td>2</td><td>Link is in the U2 State</td></tr>
<tr><td>3</td><td>Link is in the U3 State (Device Suspended)</td></tr>
<tr><td>4</td><td>Link is in the Disabled State</td></tr>
<tr><td>5</td><td>Link is in the RxDetect State</td></tr>
<tr><td>6</td><td>Link is in the Inactive State</td></tr>
<tr><td>7</td><td>Link is in the Polling State</td></tr>
<tr><td>8</td><td>Link is in the Recovery State</td></tr>
<tr><td>9</td><td>Link is in the Hot Reset State</td></tr>
<tr><td>10</td><td>Link is in the Compliance Mode State</td></tr>
<tr><td>11</td><td>Link is in the Test Mode State</td></tr>
<tr><td>12–14</td><td>Reserved</td></tr>
<tr><td>15</td><td>Link is in the Resume State</td></tr>
</table>
Notes:
1. This field is undefined if PP = 0.
2. Transitions between different states are not reflected until the transition is complete.
3. This bit is in the Suspend Well.
</td></tr>
<tr><td>4</td><td>
Port Reset (PR) — R/W. When software writes a 1 to this bit (from a 0), the bus reset sequence as defined in the USB Specification, Revision 2.0 is started. Software writes a 0 to this bit to terminate the bus reset sequence. Software must keep this bit at a 1 long enough to ensure the reset sequence completes as specified in the USB Specification, Revision 2.0. USB 3.0 ports shall execute the Hot Reset sequence as defined in the USB 3.0 Specification. PR remains set until reset signaling is completed by the root hub.
1 = Port is in Reset.
0 = Port is not in Reset.
Note: This bit is in the Suspend Well.
</td></tr>
<tr><td>3</td><td>
Overcurrent Active (OCA)— RO.
0 = This port does not have an overcurrent condition. (Default)
1 = This port currently has an overcurrent condition. This bit will automatically transition from 1 to 0 when the over current condition is removed. Intel® Xeon® Processor D-1500 Product Family automatically disables the port when the overcurrent active bit is 1.
Note: This bit is in the Suspend Well.
</td></tr>
</table>



Bit	Description
2	Reserved.
1	**Port Enabled/Disabled** — R/W. Ports can only be enabled by the host controller as a part of the reset and enable. Software cannot enable a port by writing a 1 to this bit. Ports can be disabled by either a fault condition (disconnect event or other fault condition) or by host software. The bit status does not change until the port state actually changes. There may be a delay in disabling or enabling a port due to other host controller and bus events. 0 = Disable 1 = Enable (Default) ***Note:*** This bit is in the Suspend Well.
0	**Current Connect Status** — RO. This value reflects the current state of the port, and may not correspond directly to the event that caused the Connect Status Change bit (Bit 1) to be set. 0 = No device is present. (Default) 1 = Device is present on port. ***Note:*** This bit is in the Suspend Well.

11.3.2.13 PORTPMSCN—Port N Power Management Status and Control USB3 Register

Offset: There are 6 USB3 PORTPMSCN registers at offsets: 574h, 584h, 594h, 5A4h, 5B4h, 5C4h
Attribute: R/W, RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:17	Reserved.
16	**Force Link PM Accept (FLA)** — R/W. When this bit is set to '1', the port shall generate a Set Link Function LMP with the Force_LinkPM_Accept bit asserted. This bit shall be cleared to 0b by the assertion of PR to 1 or when CCS = transitions from 0 to 1. Writes to this flag have no affect if PP = 0b. The Set Link Function LMP is sent by the xHC to the device connected on this port when this bit transitions from 0' to 1. Refer to Sections 8.4.1, 10.4.2.2 and 10.4.2.9 of the USB 3.0 Specification for more details.
15:8	**U2 Timeout** — R/W. Timeout value for U2 inactivity timer. If equal to FFh, the port is disabled from initiating U2 entry. This field shall be cleared to 0 by the assertion of PR to 1. Refer to Section 4 of the xHCI Specification for more information on U2 Timeout operation. The following are permissible values: **Value** — **Description** 00h — Zero (default) 01h — 256 µs 02h — 512 µs ... FEh — 65.024 ms FFh — Infinite
7:0	**U1 Timeout** — R/W. Timeout value for U1 inactivity timer. If equal to FFh, the port is disabled from initiating U1 entry. This field shall be cleared to 0 by the assertion of PR to 1. Refer to Section 4 of the xHCI Specification for more information on U1 Timeout operation. The following are permissible values: **Value** — **Description** 00h — Zero (default) 01h — 1 µs 02h — 2 µs ... 7Fh — 127 µs 80h-FEh — Reserved FFh — Infinite

11.3.2.14 PORTLIX— USB 3.0 Port X Link Info Register

Offset: There are 6 USB3 PORTLIX registers at offsets: 578h, 588h, 598h, 5A8h, 5B8h, 5C8h
Attribute: RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:16	**Reserved.**
15:0	**Link Error Count** - RO.

11.3.3 Host Controller Runtime Registers

This section defines the xHC runtime registers. The base address of this register space is referred to as Runtime Base. The Runtime Base shall be 32-byte aligned and is calculated by adding the value Runtime Register Space Offset register (MEM_BASE+18h:bits 31:2) to the Capability Base address. All Runtime registers are multiples of 32 bits in length.

Table 11-4. Enhanced Host Controller Operational Register Address Map

Runtime Base + Offset	Power Well	Mnemonic	Register Name	Default	Special Notes	Type
00h–03h	Core	MFINDEX	Microframe Index	00000000h		RO
20h–23h	Core	IMAN	Interrupter X Management	00000000h		RO, R/W, R/WC
24h–27h	Core	IMOD	Interrupter X Moderation	00000FA0h		R/W
28h–2Bh	Core	ERSTSZ	Event Ring Segment Table Size X	00000000h		R/W, RO
30h–33h	Core	ERSTBAL	Event Ring Segment Table Base Address Low X	00000000h		R/W, RO
34h–37h	Core	ERSTBAH	Event Ring Segment Table Base Address High X	00000000h		R/W
38h–3Bh	Core	ERDPL	Event Ring Dequeue Pointer Low X	00000000h		R/W, R/WC
3Ch–3Fh	Core	ERDPH	Event Ring Dequeue Pointer High X	00000000h		R/W

11.3.3.1 MFINDEX—Microframe Index Register

Offset: Runtime Base + 00h-03h Attribute: RO,
Default Value: 00000000h Size: 32 bits

Bit	Description
31:14	Reserved.
13:0	**Microframe Index** — RO. The value in this register increments at the end of each microframe (such as 125 us.). Bits 13:3 may be used to determine the current 1ms. Frame Index.

11.3.3.2 IMAN—Interrupter X Management Register

Offset: Interrupter 1: Runtime Base + 20h–23h
Interrupter 2: Runtime Base + 40h–43h
Interrupter 3: Runtime Base + 60h–63h
Interrupter 4: Runtime Base + 80h–83h
Interrupter 5: Runtime Base + A0h–A3h
Interrupter 6: Runtime Base + C0h–C3h
Interrupter 7: Runtime Base + E0h–E3h
Interrupter 8: Runtime Base + 100h–103h

Attribute: RO, R/W, R/WC
Default Value: 00000000h Size: 32 bits

Note: The xHC implements up to 8 Interrupters. There are 8 IMAN registers, one for each Interrupter.

Bit	Description
31:2	Reserved.
1	**Interrupt Enable (IE)** — RO. This flag specifies whether the Interrupter is capable of generating an interrupt. 0 = The Interrupter is prohibited from generating interrupts. 1 = When this bit and the IP bit are set (1b), the Interrupter shall generate an interrupt when the Interrupter Moderation Counter reaches '0'.
0	**Interrupt Pending (IP)** — R/WC. 0 = No interrupt is pending for the Interrupter. 1 = An interrupt is pending for this Interrupter. This bit is set to 1b when IE = 1, the IMODI Interrupt Moderation Counter field = 0b, the Event Ring associated with the Interrupter is not empty (or for the Primary Interrupter when the HCE flag is set to 1b), and EHB = 0. If MSI interrupts are enabled, this flag shall be cleared automatically when the PCI DWord write generated by the Interrupt assertion is complete. If PCI Pin Interrupts are enabled, this flag shall be cleared by software.

11.3.3.3 IMOD—Interrupter X Moderation Register

Offset: Interrupter 1: Runtime Base + 24h–27h
Interrupter 2: Runtime Base + 44h–47h
Interrupter 3: Runtime Base + 64h–67h
Interrupter 4: Runtime Base + 84h–87h
Interrupter 5: Runtime Base + A4h–A7h
Interrupter 6: Runtime Base + C4h–C7h
Interrupter 7: Runtime Base + E4h–E7h
Interrupter 8: Runtime Base + 104h–107h

Attribute: R/W
Default Value: 00000FA0h Size: 32 bits

Note: The xHC implements up to 8 Interrupters. There are 8 IMOD registers, one for each Interrupter.

Bit	Description
31:16	**Interrupt Moderation Counter (IMODC)** — R/W. Down counter. Loaded with Interval Moderation value (value of bits 15:0) whenever the IP bit is cleared to 0b, counts down to '0', and stops. The associated interrupt shall be signaled whenever this counter is '0', the Event Ring is not empty, the IE and IP bits = 1, and EHB = 0. This counter may be directly written by software at any time to alter the interrupt rate.
15:0	**Interrupt Moderation Interval (IMODI)** — R/W. Minimum inter-interrupt interval. The interval is specified in 250ns increments. A value of '0' disables interrupt throttling logic and interrupts shall be generated immediately if IP = 0, EHB = 0, and the Event Ring is not empty.

11.3.3.4 ERSTSZ—Event Ring Segment Table Size X Register

Offset: 1: Runtime Base + 28h–2Bh
2: Runtime Base + 48h–4Bh
3: Runtime Base + 68h–6Bh
4: Runtime Base + 88h–8Bh
5: Runtime Base + A8h–ABh
6: Runtime Base + C8h–CBh
7: Runtime Base + E8h–EBh
8: Runtime Base + 108h–10Bh

Attribute: R/W, RO
Default Value: 00000000h Size: 32 bits

Note: There are 8 ERSTSZ registers.

Bit	Description
31:16	Reserved.
15:0	**Event Ring Segment Table Size** — R/W. This field identifies the number of valid Event Ring Segment Table entries in the Event Ring Segment Table pointed to by the Event Ring Segment Table Base Address register.

11.3.3.5 ERSTBAL—Event Ring Segment Table Base Address Low X Register

Offset: 1: Runtime Base + 30h–33h
2: Runtime Base + 50h–53h
3: Runtime Base + 70h–73h
4: Runtime Base + 90h–93h
5: Runtime Base + B0h–B3h
6: Runtime Base + D0h–D3h
7: Runtime Base + F0h–F3h
8: Runtime Base + 110h–113h

Attribute: R/W, RO
Default Value: 00000000h Size: 32 bits

Note: There are 8 ERSTBAL registers.

Bit	Description
31:6	**Event Ring Segment Table Base Address Register (ERSTBA_LO)** — R/W. This field defines the low order bits of the start address of the Event Ring Segment Table. This field shall not be modified if HCHalted (HCH) = 0.
5:0	Reserved.

11.3.3.6 ERSTBAH—Event Ring Segment Table Base Address High X Register

Offset: 1: Runtime Base + 34h–37h
2: Runtime Base + 54h–57h
3: Runtime Base + 74h–77h
4: Runtime Base + 94h–97h
5: Runtime Base + B4h–B7h
6: Runtime Base + D4h–D7h
7: Runtime Base + F4h–F7h
8: 1Runtime Base + 14h–117h

Attribute: R/W
Default Value: 00000000h Size: 32 bits

Note: There are 8 ERSTBAH registers.

Bit	Description
31:0	**Event Ring Segment Table Base Address Register (ERSTBA_HI)** — R/W. This field defines the low order bits of the start address of the Event Ring Segment Table. This field shall not be modified if HCHalted (HCH) = 0.

11.3.3.7 ERDPL—Event Ring Dequeue Pointer Low X Register

Offset: 1: Runtime Base + 38h–3Bh
2: Runtime Base + 58h–5Bh
3: Runtime Base + 78h–7Bh
4: Runtime Base + 98h–9Bh
5: Runtime Base + B8h–BBh
6: Runtime Base + D8h–dBh
7: Runtime Base + F8h–FBh
8: Runtime Base + 118h–11Bh

Attribute: R/W, R/WC
Default Value: 00000000h Size: 32 bits

Note: There are 8 ERDPL registers.

Bit	Description
31:4	**Event Ring Dequeue Pointer** — R/W. This field defines the low order bits of the 64- bit address of the current Event Ring Dequeue Pointer.
3	**Event Handler Busy (EHB)** — R/WC. This flag shall be set to '1' when the IP bit is set to '1' and cleared to '0' by software when the Dequeue Pointer register is written.
2:0	**Dequeue ERST Segment Index (DESI)** — R/W. This field may be used by the xHC to accelerate checking the Event Ring full condition. This field is written with the low order 3 bits of the offset of the ERST entry which defines the Event Ring segment that Event Ring Dequeue Pointer resides in.

11.3.3.8 ERDPH—Event Ring Dequeue Pointer High X Register

Offset: 1: Runtime Base + 3Ch–3Fh
2: Runtime Base + 5Ch–5Fh
3: Runtime Base + 7Ch–7Fh
4: Runtime Base + 9Ch–9Fh
5: Runtime Base + BCh–BFh
6: Runtime Base + DCh–DFh
7: Runtime Base + FCh–FFh
8: Runtime Base + 11Ch–11Fh

Attribute: R/W
Default Value: 00000000h Size: 32 bits

Note: There are 8 ERDPH registers.

Bit	Description
31:0	**Event Ring Dequeue Pointer** — R/W. This field defines the low order bits of the 64- bit address of the current Event Ring Dequeue Pointer.

11.3.4 Doorbell Registers

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the xHC and the remainder being reserved. One 32-bit Doorbell Register is defined in the array for each Device Slot. System software utilizes the Doorbell Register to notify the xHC that it has Device Slot related work for the xHC to perform.

These registers are pointed to by the Doorbell Offset Register (dBOFF) in the xHC Capability register space. The Doorbell Array base address shall be DWord aligned and is calculated by adding the value in the dBOFF register (MEM_BASE+14h-17h) to "Base" (the base address of the xHCI Capability register address space).

All registers are 32 bits in length. Software should read and write these registers using only DWord accesses.

11.3.4.1 DOORBELL—Doorbell X Register

Offset: Doorbell 1: dBOFF + 00h-03h
Doorbell 2: dBOFF + 04h-07h
....
Doorbell 32: dBOFF + 7Ch-7Fh

Attribute: R/W
Default Value: 00000000h Size: 32 bits
Power Well Core

Note: There are 32 contiguous DOORBELL registers.

Note: Reading this register will always show 00000000h.

Bit	Description
31:16	**dB Stream ID** — R/W. If the endpoint of a Device Context Doorbell defines Streams, then this field shall be used to identify which Stream of the endpoint the doorbell reference is targeting. System software is responsible for ensuring that the value written to this field is valid. If the endpoint does not define Streams (MaxPStreams = 0) and a non-'0' value is written to this field, the doorbell reference shall be ignored. This field only applies to Device Context Doorbells and shall be cleared to '0' for Host Controller Commands. This field returns '0' when read.
15:8	Reserved.
7:0	**dB Target** — R/W. This field defines the target of the doorbell reference. The table below defines the xHC notification that is generated by ringing the doorbell. The Doorbell Register 0 is dedicated to Command Ring and decodes this field differently than the other Doorbell Registers. Refer to the xHCI Specification for definitions of the values.

§

12 SMBus Controller Registers (D31:F3)

12.1 PCI Configuration Registers (SMBus—D31:F3)

Table 12-1. SMBus Controller PCI Register Address Map (SMBus—D31:F3)

Offset	Mnemonic	Register Name	Default	Attribute
00h–01h	VID	Vendor Identification	8086	RO
02h–03h	DID	Device Identification	See register description	RO
04h–05h	PCICMD	PCI Command	0000h	R/W, RO
06h–07h	PCISTS	PCI Status	0280h	RO
08h	RID	Revision Identification	See register description	RO
09h	PI	Programming Interface	00h	RO
0Ah	SCC	Sub Class Code	05h	RO
0Bh	BCC	Base Class Code	0Ch	RO
10h	SMBMBAR0	Memory Base Address Register 0 (Bit 31:0)	00000004h	R/W, RO
14h	SMBMBAR1	Memory Based Address Register 1 (Bit 63:32)	00000000h	R/W
20h–23h	SMB_BASE	SMBus Base Address	00000001h	R/W, RO
2Ch–2Dh	SVID	Subsystem Vendor Identification	0000h	RO
2Eh–2Fh	SID	Subsystem Identification	0000h	R/WO
3Ch	INT_LN	Interrupt Line	00h	R/W
3Dh	INT_PN	Interrupt Pin	See register description	RO
40h	HOSTC	Host Configuration	00h	R/W, R/WO

Note: Registers that are not shown should be treated as Reserved (See Section 4.2 for details).

12.1.1 VID—Vendor Identification Register (SMBus—D31:F3)

Address: 00h–01h Attribute: RO
Default Value: 8086h Size: 16 bits

Bit	Description
15:0	**Vendor ID** — RO. This is a 16-bit value assigned to Intel

12.1.2 DID—Device Identification Register (SMBus—D31:F3)

Address: 02h–03h Attribute: RO
Default Value: See bit description Size: 16 bits

Bit	Description
15:0	**Device ID** — RO. This is a 16-bit value assigned to Intel® Xeon® Processor D-1500 Product Family SMBus controller.

12.1.3 PCICMD—PCI Command Register (SMBus—D31:F3)

Address: 04h–05h Attributes: RO, R/W
Default Value: 0000h Size: 16 bits

Bit	Description
15:11	Reserved
10	**Interrupt Disable** — R/W. 0 = Enable 1 = Disables SMBus to assert its PIRQB# signal.
9	Fast Back to Back Enable (FBE) — RO. Hardwired to 0.
8	**SERR# Enable (SERR_EN)** — R/W. 0 = Enables SERR# generation. 1 = Disables SERR# generation.
7	Wait Cycle Control (WCC) — RO. Hardwired to 0.
6	**Parity Error Response (PER)** — R/W. 0 = Disable 1 = Sets Detected Parity Error bit (D31:F3:06, bit 15) when a parity error is detected.
5	VGA Palette Snoop (VPS) — RO. Hardwired to 0.
4	Postable Memory Write Enable (PMWE) — RO. Hardwired to 0.
3	Special Cycle Enable (SCE) — RO. Hardwired to 0.
2	Bus Master Enable (BME) — RO. Hardwired to 0.
1	**Memory Space Enable (MSE)** — R/W. 0 = Disables memory mapped config space. 1 = Enables memory mapped config space.
0	**I/O Space Enable (IOSE)** — R/W. 0 = Disable 1 = Enables access to the SMBus I/O space registers as defined by the Base Address Register.

12.1.4 PCISTS—PCI Status Register (SMBus—D31:F3)

Address: 06h–07h Attributes: RO
Default Value: 0280h Size: 16 bits

Note: For the writable bits, software must write a 1 to clear bits that are set. Writing a 0 to the bit has no effect.

Bit	Description
15	**Detected Parity Error (DPE)** — R/WC. 0 = No parity error detected. 1 = Parity error detected.
14	**Signaled System Error (SSE)** — R/WC. 0 = No system error detected. 1 = System error detected.
13	Received Master Abort (RMA) — RO. Hardwired to 0.
12	Received Target Abort (RTA) — RO. Hardwired to 0.
11	**Signaled Target Abort (STA)** — RO. Hardwired to 0.
10:9	**DEVSEL# Timing Status** (DEVT) — RO. This 2-bit field defines the timing for DEVSEL# assertion for positive decode. 01 = Medium timing.
8	Data Parity Error Detected (DPED) — RO. Hardwired to 0.
7	Fast Back to Back Capable (FB2BC) — RO. Hardwired to 1.
6	User Definable Features (UDF) — RO. Hardwired to 0.
5	66 MHz Capable (66MHZ_CAP) — RO. Hardwired to 0.
4	**Capabilities List** (CAP_LIST) — RO. Hardwired to 0 because there are no capability list structures in this function

Bit	Description
3	**Interrupt Status (INTS)** — RO. This bit indicates that an interrupt is pending. It is independent from the state of the Interrupt Enable bit in the PCI Command register.
2:0	Reserved

12.1.5 RID—Revision Identification Register (SMBus—D31:F3)

Offset Address: 08h Attribute: RO
Default Value: See bit description Size: 8 bits

Bit	Description
7:0	**Revision ID** — RO. This field indicates the device specific revision identifier.

12.1.6 PI—Programming Interface Register (SMBus—D31:F3)

Offset Address: 09h Attribute: RO
Default Value: 00h Size: 8 bits

Bit	Description
7:0	Reserved

12.1.7 SCC—Sub Class Code Register (SMBus—D31:F3)

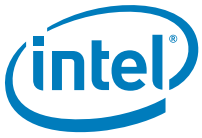
Address Offset: 0Ah Attributes: RO
Default Value: 05h Size: 8 bits

Bit	Description
7:0	**Sub Class Code** (SCC) — RO. 05h = SMBus serial controller

12.1.8 BCC—Base Class Code Register (SMBus—D31:F3)

Address Offset: 0Bh Attributes: RO
Default Value: 0Ch Size: 8 bits

Bit	Description
7:0	**Base Class Code** (BCC) — RO. 0Ch = Serial controller.



12.1.9 SMBMBAR0—D31_F3_SMBus Memory Base Address 0 Register (SMBus—D31:F3)

Address Offset: 10–13h
Default Value: 00000004h
Attributes: R/W, RO
Size: 32 bits

Bit	Description
31:8	**Base Address** — R/W. Provides the 32 byte system memory base address for Intel® Xeon® Processor D-1500 Product Family SMB logic.
7:4	Reserved
3	Prefetchable (PREF) — RO. Hardwired to 0. Indicates that SMBMBAR is not pre-fetchable.
2:1	**Address Range (ADDRNG)** — RO. Indicates that this SMBMBAR can be located anywhere in 64 bit address space. Hardwired to 10b.
0	**Memory Space Indicator** — RO. This read-only bit always is 0, indicating that the SMB logic is Memory mapped.

12.1.10 SMBMBAR1—D31_F3_SMBus Memory Base Address 1 Register (SMBus—D31:F3)

Address Offset: 14h–17h
Default Value: 00000000h
Attributes: R/W
Size: 32 bits

Bit	Description
31:0	**Base Address** — R/W. Provides bits 63:32 system memory base address for Intel® Xeon® Processor D-1500 Product Family SMB logic.

12.1.11 SMB_BASE—SMBus Base Address Register (SMBus—D31:F3)

Address Offset: 20–23h
Default Value: 00000001h
Attribute: R/W, RO
Size: 32-bits

Bit	Description
31:16	Reserved — RO
15:5	**Base Address** — R/W. This field provides the 32-byte system I/O base address for Intel® Xeon® Processor D-1500 Product Family's SMB logic.
4:1	Reserved — RO
0	IO Space Indicator — RO. Hardwired to 1 indicating that the SMB logic is I/O mapped.

12.1.12 SVID—Subsystem Vendor Identification Register (SMBus—D31:F2/F4)

Address Offset: 2Ch–2Dh
Default Value: 0000h
Lockable: No
Attribute: RO
Size: 16 bits
Power Well: Core

Bit	Description
15:0	**Subsystem Vendor ID (SVID)** — RO. The SVID register, in combination with the Subsystem ID (SID) register, enables the operating system (OS) to distinguish subsystems from each other. The value returned by reads to this register is the same as that which was written by BIOS into the IDE SVID register. ***Note:*** Software can write to this register only once per core well reset. Writes should be done as a single 16-bit cycle.

12.1.13 SID—Subsystem Identification Register (SMBus—D31:F2/F4)

Address Offset:	2Eh–2Fh	Attribute:	R/WO
Default Value:	0000h	Size:	16 bits
Lockable:	No	Power Well:	Core

Bit	Description
15:0	**Subsystem ID (SID)** — R/WO. The SID register, in combination with the SVID register, enables the operating system (OS) to distinguish subsystems from each other. The value returned by reads to this register is the same as that which was written by BIOS into the IDE SID register. ***Note:*** Software can write to this register only once per core well reset. Writes should be done as a single 16-bit cycle.

12.1.14 INT_LN—Interrupt Line Register (SMBus—D31:F3)

Address Offset:	3Ch	Attributes:	R/W
Default Value:	00h	Size:	8 bits

Bit	Description
7:0	**Interrupt Line (INT_LN)** — R/W. This data is not used by Intel® Xeon® Processor D-1500 Product Family. It is to communicate to software the interrupt line that the interrupt pin is connected to PIRQB#.

12.1.15 INT_PN—Interrupt Pin Register (SMBus—D31:F3)

Address Offset:	3Dh	Attributes:	RO
Default Value:	See description	Size:	8 bits

Bit	Description
7:0	**Interrupt PIN (INT_PN)** — RO. This reflects the value of D31IP.SMIP in chipset configuration space.

12.1.16 HOSTC—Host Configuration Register (SMBus—D31:F3)

Address Offset:	40h	Attribute:	R/W, R/WO
Default Value:	00h	Size:	8 bits

Bit	Description
7:5	Reserved
4	**SPD Write Disable** — R/WO. 0 = SPD write enabled. 1 = SPD write disabled. Writes to SMBus addresses 50h - 57h are disabled. ***Note:*** This bit is R/WO and will be reset on PLTRST# assertion. This bit should be set by BIOS to '1'. SW can only program this bit when both the START bit (SMB_BASE + 02h, bit 6) and Host Busy bit (SMB_BASE + 00h, bit 0) are '0'; otherwise the write may result in undefined behavior.
3	**Soft SMBus Reset (SSRESET)** — R/W. 0 = The HW will reset this bit to 0 when SMBus reset operation is completed. 1 = The SMBus state machine and logic in Intel® Xeon® Processor D-1500 Product Family is reset.
2	**I^2C_EN** — R/W. 0 = SMBus behavior. 1 = Intel® Xeon® Processor D-1500 Product Family is enabled to communicate with I^2C devices. This will change the formatting of some commands.
1	**SMB_SMI_EN** — R/W. 0 = SMBus interrupts will not generate an SMI#. 1 = Any source of an SMB interrupt will instead be routed to generate an SMI#. Refer to Section 3.20.4 (Interrupts / SMI#). This bit needs to be set for SMBALERT# to be enabled.

Bit	Description
0	**SMBus Host Enable (HST_EN)** — R/W. 0 = Disable the SMBus Host controller. 1 = Enable. The SMB Host controller interface is enabled to execute commands. The INTREN bit (offset SMB_BASE + 02h, bit 0) needs to be enabled for the SMB Host controller to interrupt or SMI#. The SMB Host controller will not respond to any new requests until all interrupt requests have been cleared.

12.2 SMBus I/O and Memory Mapped I/O Registers

The SMBus registers (see Table 12-2) can be accessed through I/O BAR or Memory BAR registers in PCI configuration space. The offsets are the same for both I/O and Memory Mapped I/O registers.

Table 12-2. SMBus I/O and Memory Mapped I/O Register Address Map

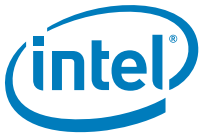
SMB_BASE + Offset	Mnemonic	Register Name	Default	Attribute
00h	HST_STS	Host Status	00h	R/WC, RO
02h	HST_CNT	Host Control	00h	R/W, WO
03h	HST_CMD	Host Command	00h	R/W
04h	XMIT_SLVA	Transmit Slave Address	00h	R/W
05h	HST_D0	Host Data 0	00h	R/W
06h	HST_D1	Host Data 1	00h	R/W
07h	HOST_BLOCK_dB	Host Block Data Byte	00h	R/W
08h	PEC	Packet Error Check	00h	R/W
09h	RCV_SLVA	Receive Slave Address	44h	R/W
0Ah–0Bh	SLV_DATA	Receive Slave Data	0000h	RO
0Ch	AUX_STS	Auxiliary Status	00h	R/WC, RO
0Dh	AUX_CTL	Auxiliary Control	00h	R/W
0Eh	SMLINK_PIN_CTL	SMLink Pin Control (TCO Compatible Mode)	See register description	R/W, RO
0Fh	SMBus_PIN_CTL	SMBus Pin Control	See register description	R/W, RO
10h	SLV_STS	Slave Status	00h	R/WC
11h	SLV_CMD	Slave Command	00h	R/W
14h	NOTIFY_DADDR	Notify Device Address	00h	RO
16h	NOTIFY_DLOW	Notify Data Low Byte	00h	RO
17h	NOTIFY_DHIGH	Notify Data High Byte	00h	RO

12.2.1 HST_STS—Host Status Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 00h	Attribute:	R/WC, RO
Default Value:	00h	Size:	8-bits

All status bits are set by hardware and cleared by the software writing a one to the particular bit position. Writing a 0 to any bit position has no effect.

Bit	Description
7	**Byte Done Status (DS)** — R/WC. 0 = Software can clear this by writing a 1 to it. 1 = Host controller received a byte (for Block Read commands) or if it has completed transmission of a byte (for Block Write commands) when the 32-byte buffer is not being used. This bit will be set, even on the last byte of the transfer. This bit is not set when transmission is due to the LAN interface heartbeat. This bit has no meaning for block transfers when the 32-byte buffer is enabled. ***Note:*** When the last byte of a block message is received, the host controller will set this bit. However, it will not immediately set the INTR bit (bit 1 in this register). When the interrupt handler clears the DS bit, the message is considered complete, and the host controller will then set the INTR bit (and generate another interrupt). Thus, for a block message of n bytes, Intel® Xeon® Processor D-1500 Product Family will generate n+1 interrupts. The interrupt handler needs to be implemented to handle these cases. When not using the 32 Byte Buffer, hardware will drive the SMBCLK signal low when the DS bit is set until SW clears the bit. This includes the last byte of a transfer. Software must clear the DS bit before it can clear the BUSY bit.
6	**INUSE_STS** — R/W. This bit is used as semaphore among various independent software threads that may need to use Intel® Xeon® Processor D-1500 Product Family's SMBus logic, and has no other effect on hardware. 0 = After a full PCI reset, a read to this bit returns a 0. 1 = After the first read, subsequent reads will return a 1. A write of a 1 to this bit will reset the next read value to 0. Writing a 0 to this bit has no effect. Software can poll this bit until it reads a 0, and will then own the usage of the host controller.
5	**SMBALERT_STS** — R/WC. 0 = Interrupt or SMI# was not generated by SMBALERT#. Software clears this bit by writing a 1 to it. 1 = The source of the interrupt or SMI# was the SMBALERT# signal. This bit is only cleared by software writing a 1 to the bit position or by RSMRST# going low. If the signal is programmed as a GPIO, then this bit will never be set.
4	**FAILED** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = The source of the interrupt or SMI# was a failed bus transaction. This bit is set in response to the KILL bit being set to terminate the host transaction.
3	**BUS_ERR** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = The source of the interrupt of SMI# was a transaction collision.
2	**DEV_ERR** — R/WC. 0 = Software clears this bit by writing a 1 to it. Intel® Xeon® Processor D-1500 Product Family will then de-assert the interrupt or SMI#. 1 = The source of the interrupt or SMI# was due to one of the following: • Invalid Command Field, • Unclaimed Cycle (host initiated), • Host Device Time-out Error.
1	**INTR** — R/WC. This bit can only be set by termination of a command. INTR is not dependent on the INTREN bit (offset SMB_BASE + 02h, bit 0) of the Host controller register (offset 02h). It is only dependent on the termination of the command. If the INTREN bit is not set, then the INTR bit will be set, although the interrupt will not be generated. Software can poll the INTR bit in this non-interrupt case. 0 = Software clears this bit by writing a 1 to it. Intel® Xeon® Processor D-1500 Product Family then de-asserts the interrupt or SMI#. 1 = The source of the interrupt or SMI# was the successful completion of its last command.



Bit	Description
0	**HOST_BUSY** — R/WC. 0 = Cleared by Intel® Xeon® Processor D-1500 Product Family when the current transaction is completed. 1 = Indicates that Intel® Xeon® Processor D-1500 Product Family is running a command from the host interface. No SMB registers should be accessed while this bit is set, except the BLOCK DATA BYTE Register. The BLOCK DATA BYTE Register can be accessed when this bit is set only when the SMB_CMD bits in the Host Control Register are programmed for Block command or I^2C Read command. This is necessary in order to check the DONE_STS bit.

12.2.2 HST_CNT—Host Control Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 02h	Attribute:	R/W, WO
Default Value:	00h	Size:	8-bits

Note: A read to this register will clear the byte pointer of the 32-byte buffer.

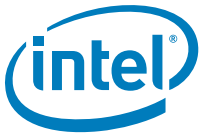
Bit	Description
7	**PEC_EN** — R/W. 0 = SMBus host controller does not perform the transaction with the PEC phase appended. 1 = Causes the host controller to perform the SMBus transaction with the Packet Error Checking phase appended. For writes, the value of the PEC byte is transferred from the PEC Register. For reads, the PEC byte is loaded in to the PEC Register. This bit must be written prior to the write in which the **START** bit is set.
6	**START** — WO. 0 = This bit will always return 0 on reads. The HOST_BUSY bit in the Host Status register (offset 00h) can be used to identify when Intel® Xeon® Processor D-1500 Product Family has finished the command. 1 = Writing a 1 to this bit initiates the command described in the SMB_CMD field. All registers should be setup prior to writing a 1 to this bit position.
5	**LAST_BYTE** — WO. This bit is used for Block Read commands. 1 = Software sets this bit to indicate that the next byte will be the last byte to be received for the block. This causes Intel® Xeon® Processor D-1500 Product Family to send a NACK (instead of an ACK) after receiving the last byte. ***Note:*** Once the SECOND_TO_STS bit in TCO2_STS register (D31:F0, TCOBASE+6h, bit 1) is set, the LAST_BYTE bit also gets set. While the SECOND_TO_STS bit is set, the LAST_BYTE bit cannot be cleared. This prevents Intel® Xeon® Processor D-1500 Product Family from running some of the SMBus commands (Block Read/Write, I^2C Read, Block I^2C Write).

Bit	Description
4:2	**SMB_CMD** — R/W. The bit encoding below indicates which command Intel® Xeon® Processor D-1500 Product Family is to perform. If enabled, Intel® Xeon® Processor D-1500 Product Family will generate an interrupt or SMI# when the command has completed If the value is for a non-supported or reserved command, Intel® Xeon® Processor D-1500 Product Family will set the device error (DEV_ERR) status bit (offset SMB_BASE + 00h, bit 2) and generate an interrupt when the START bit is set. Intel® Xeon® Processor D-1500 Product Family will perform no command, and will not operate until DEV_ERR is cleared. 000 = **Quick**: The slave address and read/write value (bit 0) are stored in the transmit slave address register. 001 = **Byte**: This command uses the transmit slave address and command registers. Bit 0 of the slave address register determines if this is a read or write command. 010 = **Byte Data**: This command uses the transmit slave address, command, and DATA0 registers. Bit 0 of the slave address register determines if this is a read or write command. If it is a read, the DATA0 register will contain the read data. 011 = **Word Data**: This command uses the transmit slave address, command, DATA0 and DATA1 registers. Bit 0 of the slave address register determines if this is a read or write command. If it is a read, after the command completes, the DATA0 and DATA1 registers will contain the read data. 100 = **Process Call:** This command uses the transmit slave address, command, DATA0 and DATA1 registers. Bit 0 of the slave address register determines if this is a read or write command. After the command completes, the DATA0 and DATA1 registers will contain the read data. 101 = **Block**: This command uses the transmit slave address, command, DATA0 registers, and the Block Data Byte register. For block write, the count is stored in the DATA0 register and indicates how many bytes of data will be transferred. For block reads, the count is received and stored in the DATA0 register. Bit 0 of the slave address register selects if this is a read or write command. For writes, data is retrieved from the first n (where n is equal to the specified count) addresses of the SRAM array. For reads, the data is stored in the Block Data Byte register. 110 = **I^2C Read**: This command uses the transmit slave address, command, DATA0, DATA1 registers, and the Block Data Byte register. The read data is stored in the Block Data Byte register. Intel® Xeon® Processor D-1500 Product Family continues reading data until the NAK is received. 111 **= Block Process:** This command uses the transmit slave address, command, DATA0 and the Block Data Byte register. For block write, the count is stored in the DATA0 register and indicates how many bytes of data will be transferred. For block read, the count is received and stored in the DATA0 register. Bit 0 of the slave address register always indicate a write command. For writes, data is retrieved from the first m (where m is equal to the specified count) addresses of the SRAM array. For reads, the data is stored in the Block Data Byte register. ***Note:*** E32B bit in the Auxiliary Control register must be set for this command to work.
1	**KILL** — R/W. 0 = Normal SMBus host controller functionality. 1 = Kills the current host transaction taking place, sets the FAILED status bit, and asserts the interrupt (or SMI#). This bit, once set, must be cleared by software to allow the SMBus host controller to function normally.
0	**INTREN** — R/W. 0 = Disable. 1 = Enable the generation of an interrupt or SMI# upon the completion of the command.

12.2.3 HST_CMD—Host Command Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 03h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

Bit	Description
7:0	This 8-bit field is transmitted by the host controller in the command field of the SMBus protocol during the execution of any command.



12.2.4 XMIT_SLVA—Transmit Slave Address Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 04h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register is transmitted by the host controller in the slave address field of the SMBus protocol.

Bit	Description
7:1	**Address** — R/W. This field provides a 7-bit address of the targeted slave.
0	**RW** — R/W. Direction of the host transfer. 0 = Write 1 = Read ***Note:*** Writes to SMBus addresses 50h - 57h are disabled depending on the setting of bit 4 in HOSTC register (D31:F3:Offset 40h).

12.2.5 HST_D0—Host Data 0 Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 05h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

Bit	Description
7:0	**Data0/Count** — R/W. This field contains the 8-bit data sent in the DATA0 field of the SMBus protocol. For block write commands, this register reflects the number of bytes to transfer. This register should be programmed to a value between 1 and 32 for block counts. A count of 0 or a count above 32 will result in unpredictable behavior. The host controller does not check or log invalid block counts.

12.2.6 HST_D1—Host Data 1 Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 06h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

Bit	Description
7:0	**Data1** — R/W. This 8-bit register is transmitted in the DATA1 field of the SMBus protocol during the execution of any command.

12.2.7 Host_BLOCK_dB—Host Block Data Byte Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 07h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

Bit	Description
7:0	**Block Data (BDTA)** — R/W. This is either a register, or a pointer into a 32-byte block array, depending upon whether the E32B bit is set in the Auxiliary Control register. When the E32B bit (offset SMB_BASE + 0Dh, bit 1) is cleared, this is a register containing a byte of data to be sent on a block write or read from on a block read. When the E32B bit is set, reads and writes to this register are used to access the 32-byte block data storage array. An internal index pointer is used to address the array, which is reset to 0 by reading the HCTL register (offset 02h). The index pointer then increments automatically upon each access to this register. The transfer of block data into (read) or out of (write) this storage array during an SMBus transaction always starts at index address 0. When the E2B bit is set, for writes, software will write up to 32-bytes to this register as part of the setup for the command. After the Host controller has sent the Address, Command, and Byte Count fields, it will send the bytes in the SRAM pointed to by this register. When the E2B bit is cleared for writes, software will place a single byte in this register. After the host controller has sent the address, command, and byte count fields, it will send the byte in this register. If there is more data to send, software will write the next series of bytes to the SRAM pointed to by this register and clear the DONE_STS bit. The controller will then send the next byte. During the time between the last byte being transmitted to the next byte being transmitted, the controller will insert wait-states on the interface. When the E2B bit is set for reads, after receiving the byte count into the Data0 register, the first series of data bytes go into the SRAM pointed to by this register. If the byte count has been exhausted or the 32-byte SRAM has been filled, the controller will generate an SMI# or interrupt (depending on configuration) and set the DONE_STS bit. Software will then read the data. During the time between when the last byte is read from the SRAM to when the DONE_STS bit is cleared, the controller will insert wait-states on the interface.

12.2.8 PEC—Packet Error Check (PEC) Register (SMBus—D31:F3)

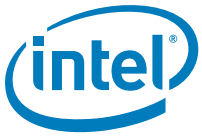
Register Offset:	SMB_BASE + 08h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

Bit	Description
7:0	**PEC_DATA** — R/W. This 8-bit register is written with the 8-bit CRC value that is used as the SMBus PEC data prior to a write transaction. For read transactions, the PEC data is loaded from the SMBus into this register and is then read by software. Software must ensure that the INUSE_STS bit is properly maintained to avoid having this field over-written by a write transaction following a read transaction.

12.2.9 RCV_SLVA—Receive Slave Address Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 09h	Attribute:	R/W
Default Value:	44h	Size:	8 bits
Lockable:	No	Power Well:	Resume

Bit	Description
7	Reserved
6:0	**SLAVE_ADDR** — R/W. This field is the slave address that Intel® Xeon® Processor D-1500 Product Family decodes for read and write cycles. the default is not 0, so the SMBus Slave Interface can respond even before the processor comes up (or if the processor is dead). This register is cleared by RSMRST#, but not by PLTRST#.



12.2.10 SLV_DATA—Receive Slave Data Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 0Ah–0Bh	Attribute:	RO
Default Value:	0000h	Size:	16 bits
Lockable:	No	Power Well:	Resume

This register contains the 16-bit data value written by the external SMBus master. The processor can then read the value from this register. This register is reset by RSMRST#, but not PLTRST#.

Bit	Description
15:8	**Data Message Byte 1 (DATA_MSG1)** — RO. See Section 3.20.7 for a discussion of this field.
7:0	**Data Message Byte 0 (DATA_MSG0)** — RO. See Section 3.20.7 for a discussion of this field.

12.2.11 AUX_STS—Auxiliary Status Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 0Ch	Attribute:	R/WC, RO
Default Value:	00h	Size:	8 bits
Lockable:	No	Power Well:	Resume

Bit	Description
7:2	Reserved
1	**SMBus TCO Mode (STCO)** — RO. This bit reflects the strap setting of TCO compatible mode versus Advanced TCO mode. 0 = Intel® Xeon® Processor D-1500 Product Family is in the compatible TCO mode. 1 = Intel® Xeon® Processor D-1500 Product Family is in the advanced TCO mode.
0	**CRC Error (CRCE)** — R/WC. 0 = Software clears this bit by writing a 1 to it. 1 = This bit is set if a received message contained a CRC error. When this bit is set, the DERR bit of the host status register will also be set. This bit will be set by the controller if a software abort occurs in the middle of the CRC portion of the cycle or an abort happens after Intel® Xeon® Processor D-1500 Product Family has received the final data bit transmitted by an external slave.

12.2.12 AUX_CTL—Auxiliary Control Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 0Dh	Attribute:	R/W
Default Value:	00h	Size:	8 bits
Lockable:	No	Power Well:	Resume

Bit	Description
7:2	Reserved
1	**Enable 32-Byte Buffer (E32B)** — R/W. 0 = Disable. 1 = Enable. When set, the Host Block Data register is a pointer into a 32-byte buffer, as opposed to a single register. This enables the block commands to transfer or receive up to 32-bytes before Intel® Xeon® Processor D-1500 Product Family generates an interrupt.
0	**Automatically Append CRC (AAC)** — R/W. 0 = Intel® Xeon® Processor D-1500 Product Family will Not automatically append the CRC. 1 = Intel® Xeon® Processor D-1500 Product Family will automatically append the CRC. This bit must not be changed during SMBus transactions or undetermined behavior will result. It should be programmed only once during the lifetime of the function.

12.2.13 SMLINK_PIN_CTL—SMLink Pin Control Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 0Eh	Attribute:	R/W, RO
Default Value:	See Description	Size:	8 bits

Note: This register is in the resume well and is reset by RSMRST#.

This register is only applicable in the TCO compatible mode.

Bit	Description
7:3	Reserved
2	**SMLINK_CLK_CTL** — R/W. 0 = Intel® Xeon® Processor D-1500 Product Family will drive the SMLink0 pin low, independent of what the other SMLink logic would otherwise indicate for the SMLink0 pin. 1 = The SMLink0 pin is **not** overdriven low. The other SMLink logic controls the state of the pin. (Default)
1	**SMLINK1_CUR_STS** — RO. This read-only bit has a default value that is dependent on an external signal level. This pin returns the value on the SMLink1 pin. This allows software to read the current state of the pin. 0 = Low 1 = High
0	**SMLINK0_CUR_STS** — RO. This read-only bit has a default value that is dependent on an external signal level. This pin returns the value on the SMLink0 pin. This allows software to read the current state of the pin. 0 = Low 1 = High

12.2.14 SMBus_PIN_CTL—SMBus Pin Control Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 0Fh	Attribute:	R/W, RO
Default Value:	See Description	Size:	8 bits

Note: This register is in the resume well and is reset by RSMRST#.

Bit	Description
7:3	Reserved
2	**SMBCLK_CTL** — R/W. 1 = The SMBCLK pin is **not** overdriven low. The other SMBus logic controls the state of the pin. 0 = Intel® Xeon® Processor D-1500 Product Family drives the SMBCLK pin low, independent of what the other SMB logic would otherwise indicate for the SMBCLK pin. (Default)
1	**SMBDATA_CUR_STS** — RO. This read-only bit has a default value that is dependent on an external signal level. This pin returns the value on the SMBDATA pin. This allows software to read the current state of the pin. 0 = Low 1 = High
0	**SMBCLK_CUR_STS** — RO. This read-only bit has a default value that is dependent on an external signal level. This pin returns the value on the SMBCLK pin. This allows software to read the current state of the pin. 0 = Low 1 = High

12.2.15 SLV_STS—Slave Status Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 10h	Attribute:	R/WC
Default Value:	00h	Size:	8 bits

Note: This register is in the resume well and is reset by RSMRST#.

All bits in this register are implemented in the 64 kHz clock domain. Therefore, software must poll this register until a write takes effect before assuming that a write has completed internally.

Bit	Description
7:1	Reserved
0	**HOST_NOTIFY_STS** — R/WC. Intel® Xeon® Processor D-1500 Product Family sets this bit to a 1 when it has completely received a successful Host Notify Command on the SMBus pins. Software reads this bit to determine that the source of the interrupt or SMI# was the reception of the Host Notify Command. Software clears this bit after reading any information needed from the Notify address and data registers by writing a 1 to this bit. Intel® Xeon® Processor D-1500 Product Family will allow the Notify Address and Data registers to be over-written once this bit has been cleared. When this bit is 1, Intel® Xeon® Processor D-1500 Product Family will NACK the first byte (host address) of any new “Host Notify” commands on the SMBus pins. Writing a 0 to this bit has no effect.

12.2.16 SLV_CMD—Slave Command Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 11h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

Note: This register is in the resume well and is reset by RSMRST#.

Bit	Description
7:2	Reserved
2	**SMBALERT_DIS** — R/W. 0 = Allows the generation of the interrupt or SMI#. 1 = Software sets this bit to block the generation of the interrupt or SMI# due to the SMBALERT# source. This bit is logically inverted and ANDed with the SMBALERT_STS bit (offset SMB_BASE + 00h, bit 5). The resulting signal is distributed to the SMI# and/or interrupt generation logic. This bit does not effect the wake logic.
1	**HOST_NOTIFY_WKEN** — R/W. Software sets this bit to 1 to enable the reception of a Host Notify command as a wake event. When enabled this event is “OR’d" in with the other SMBus wake events and is reflected in the SMB_WAK_STS bit of the General Purpose Event 0 Status register. 0 = Disable 1 = Enable
0	**HOST_NOTIFY_INTREN** — R/W. Software sets this bit to 1 to enable the generation of interrupt or SMI# when HOST_NOTIFY_STS (offset SMB_BASE + 10h, bit 0) is 1. This enable does not affect the setting of the HOST_NOTIFY_STS bit. When the interrupt is generated, either PIRQB# or SMI# is generated, depending on the value of the SMB_SMI_EN bit (D31:F3:40h, bit 1). If the HOST_NOTIFY_STS bit is set when this bit is written to a 1, then the interrupt (or SMI#) will be generated. The interrupt (or SMI#) is logically generated by AND’ing the STS and INTREN bits. 0 = Disable 1 = Enable

12.2.17 NOTIFY_DADDR—Notify Device Address Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 14h	Attribute:	RO
Default Value:	00h	Size:	8 bits

Note: This register is in the resume well and is reset by RSMRST#.

Bit	Description
7:1	**DEVICE_ADDRESS** — RO. This field contains the 7-bit device address received during the Host Notify protocol of the SMBus 2.0 Specification. Software should only consider this field valid when the HOST_NOTIFY_STS bit (D31:F3:SMB_BASE +10, bit 0) is set to 1.
0	Reserved

12.2.18 NOTIFY_DLOW—Notify Data Low Byte Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 16h	Attribute:	RO
Default Value:	00h	Size:	8 bits

Note: This register is in the resume well and is reset by RSMRST#.

Bit	Description
7:0	**DATA_LOW_BYTE** — RO. This field contains the first (low) byte of data received during the Host Notify protocol of the SMBus 2.0 specification. Software should only consider this field valid when the HOST_NOTIFY_STS bit (D31:F3:SMB_BASE +10, bit 0) is set to 1.

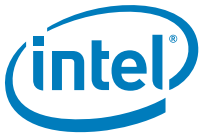
12.2.19 NOTIFY_DHIGH—Notify Data High Byte Register (SMBus—D31:F3)

Register Offset:	SMB_BASE + 17h	Attribute:	RO
Default Value:	00h	Size:	8 bits

Note: This register is in the resume well and is reset by RSMRST#.

Bit	Description
7:0	**DATA_HIGH_BYTE** — RO. This field contains the second (high) byte of data received during the Host Notify protocol of the SMBus 2.0 specification. Software should only consider this field valid when the HOST_NOTIFY_STS bit (D31:F3:SMB_BASE +10, bit 0) is set to 1.

§



13 PCI Express* Configuration Registers

13.1 PCI Express* Configuration Registers (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Note: This section assumes the default PCI Express Function Number-to-Root Port mapping is used. Function numbers for a given root port are assignable through the Root Port Function Number and Hide for PCI Express Root Ports register (RCBA+0404h).

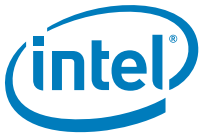
Note: Register address locations that are not shown in Table 13-1 should be treated as Reserved.

Table 13-1. PCI Express* Configuration Registers Address Map (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) (Sheet 1 of 2)

Offset	Mnemonic	Register Name	Function 0–7 Default	Attribute
00h–01h	VID	Vendor Identification	8086h	RO
02h–03h	DID	Device Identification	See register description	RO
04h–05h	PCICMD	PCI Command	0000h	R/W, RO
06h–07h	PCISTS	PCI Status	0010h	R/WC, RO
08h	RID	Revision Identification	See register description	RO
09h	PI	Programming Interface	00h	RO
0Ah	SCC	Sub Class Code	04h	RO
0Bh	BCC	Base Class Code	06h	RO
0Ch	CLS	Cache Line Size	00h	R/W
0Dh	PLT	Primary Latency Timer	00h	RO
0Eh	HEADTYP	Header Type	81h	RO
18h–1Ah	BNUM	Bus Number	000000h	R/W
1Bh	SLT	Secondary Latency Timer	00h	RO
1Ch–1Dh	IOBL	I/O Base and Limit	0000h	R/W, RO
1Eh–1Fh	SSTS	Secondary Status Register	0000h	R/WC
20h–23h	MBL	Memory Base and Limit	00000000h	R/W
24h–27h	PMBL	Prefetchable Memory Base and Limit	00010001h	R/W, RO
28h–2Bh	PMBU32	Prefetchable Memory Base Upper 32 Bits	00000000h	R/W
2Ch–2Fh	PMLU32	Prefetchable Memory Limit Upper 32 Bits	00000000h	R/W
34h	CAPP	Capabilities List Pointer	40h	RO
3Ch–3Dh	INTR	Interrupt Information	See bit description	R/W, RO
3Eh–3Fh	BCTRL	Bridge Control Register	0000h	R/W
40h–41h	CLIST	Capabilities List	8010h	RO
42h–43h	XCAP	PCI Express* Capabilities	0042h	R/WO, RO
44h–47h	DCAP	Device Capabilities	00008000h	RO
48h–49h	DCTL	Device Control	0000h	R/W, RO

Table 13-1. PCI Express* Configuration Registers Address Map (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7) (Sheet 2 of 2)

Offset	Mnemonic	Register Name	Function 0–7 Default	Attribute
4Ah–4Bh	DSTS	Device Status	0010h	R/WC, RO
4Ch–4Fh	LCAP	Link Capabilities	See bit description	RO, R/WO
50h–51h	LCTL	Link Control	0000h	R/W, RO
52h–53h	LSTS	Link Status	See bit description	RO
54h–57h	SLCAP	Slot Capabilities Register	00060060h	R/WO, RO
58h–59h	SLCTL	Slot Control	0000h	R/W, RO
5Ah–5Bh	SLSTS	Slot Status	0000h	R/WC, RO
5Ch–5Dh	RCTL	Root Control	0000h	R/W
60h–63h	RSTS	Root Status	00000000h	R/WC, RO
64h–67h	DCAP2	Device Capabilities 2 Register	00080816h	R/WO,RO
68h–69h	DCTL2	Device Control 2 Register	0000h	R/W, RO
70h–71h	LCTL2	Link Control 2 Register	0002h	R/W
72h–73h	LSTS2	Link Status 2 Register	0000h	RO
80h–81h	MID	Message Signaled Interrupt Identifiers	9005h	RO
82h–83h	MC	Message Signaled Interrupt Message Control	0000h	R/W, RO
84h–87h	MA	Message Signaled Interrupt Message Address	00000000h	R/W
88h–89h	MD	Message Signaled Interrupt Message Data	0000h	R/W
90h–91h	SVCAP	Subsystem Vendor Capability	A00Dh	R/WO,RO
94h–97h	SVID	Subsystem Vendor Identification	00000000h	R/WO
A0h–A1h	PMCAP	Power Management Capability	0001h	RO
A2h–A3h	PMC	PCI Power Management Capability	C803h	RO
A4h–A7h	PMCS	PCI Power Management Control and Status	00000000h	R/W, RO
D4h–D7h	MPC2	Miscellaneous Port Configuration 2	00000800h	R/W, RO
D8h–dBh	MPC	Miscellaneous Port Configuration	09110000h	R/W, RO, R/WO
DCh–DFh	SMSCS	SMI/SCI Status Register	00000000h	R/WC
E1h	RPDCGEN	Rort Port Dynamic Clock Gating Enable	00h	R/W
ECh–EFh	PECR3	PCI Express Configuration Register 3	00000000h	R/W
104h–107h	UES	Uncorrectable Error Status	See bit description	R/WC, RO
108h–10Bh	UEM	Uncorrectable Error Mask	00000000h	R/WO, RO
10Ch–10Fh	UEV	Uncorrectable Error Severity	00060011h	RO
110h–113h	CES	Correctable Error Status	00000000h	R/WC
114h–117h	CEM	Correctable Error Mask	00002000h	R/WO
118h–11Bh	AECC	Advanced Error Capabilities and Control	00000000h	RO
130h–133h	RES	Root Error Status	00000000h	R/WC, RO
320h–323h	PECR2	PCI Express Configuration Register 2	0004B05Bh	R/W
324h–327h	PEETM	PCI Express Extended Test Mode Register	See bit description	RO
330h–333h	PEC1	PCI Express Configuration Register 1	28000016h	RO, R/W



13.1.1 VID—Vendor Identification Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 00h–01h
Default Value: 8086h
Attribute: RO
Size: 16 bits

Bit	Description
15:0	**Vendor ID** — RO. This is a 16-bit value assigned to Intel. Intel VID = 8086h

13.1.2 DID—Device Identification Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 02h–03h
Default Value: Port 1= Bit Description
Port 2= Bit Description
Port 3= Bit Description
Port 4= Bit Description
Port 5= Bit Description
Port 6= Bit Description
Port 7= Bit Description
Port 8= Bit Description
Attribute: RO
Size: 16 bits

Bit	Description
15:0	**Device ID** — RO. This is a 16-bit value assigned to Intel® Xeon® Processor D-1500 Product Family's PCI Express controller.

13.1.3 PCICMD—PCI Command Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 04h–05h
Default Value: 0000h
Attribute: R/W, RO
Size: 16 bits

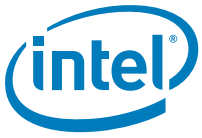
Bit	Description
15:11	Reserved
10	**Interrupt Disable** — R/W. This disables pin-based INTx# interrupts on enabled Hot-Plug and power management events. This bit has no effect on MSI operation. 0 = Internal INTx# messages are generated if there is an interrupt for Hot-Plug or power management and MSI is not enabled. 1 = Internal INTx# messages will not be generated. This bit does not affect interrupt forwarding from devices connected to the root port. Assert_INTx and Deassert_INTx messages will still be forwarded to the internal interrupt controllers if this bit is set.
9	**Fast Back to Back Enable (FBE)** — Reserved per the *PCI Express* Base Specification*.
8	**SERR# Enable (SEE)** — R/W. 0 = Disable. 1 = Enables the root port to generate an SERR# message when PSTS.SSE is set.
7	Wait Cycle Control (WCC) — Reserved per the *PCI Express Base Specification*.
6	**Parity Error Response (PER)** — R/W. 0 = Disable. 1 = Indicates that the device is capable of reporting parity errors as a master on the backbone.
5	**VGA Palette Snoop (VPS)** — Reserved per the *PCI Express* Base Specification*.
4	**Postable Memory Write Enable (PMWE)** — Reserved per the *PCI Express* Base Specification*.
3	Special Cycle Enable (SCE) — Reserved per the *PCI Express* Base Specification*.

Bit	Description
2	**Bus Master Enable (BME)** — R/W. 0 = Disable. Memory and I/O requests received at a Root Port must be handled as Unsupported Requests. 1 = Enable. Allows the root port to forward Memory and I/O Read/Write cycles onto the backbone from a PCI Express* device. ***Note:*** This bit does not affect forwarding of completions in either upstream or downstream direction nor controls forwarding of requests other than memory or I/O
1	**Memory Space Enable (MSE)** — R/W. 0 = Disable. Memory cycles within the range specified by the memory base and limit registers are master aborted on the backbone. 1 = Enable. Allows memory cycles within the range specified by the memory base and limit registers can be forwarded to the PCI Express device.
0	**I/O Space Enable (IOSE)** — R/W. This bit controls access to the I/O space registers. 0 = Disable. I/O cycles within the range specified by the I/O base and limit registers are master aborted on the backbone. 1 = Enable. Allows I/O cycles within the range specified by the I/O base and limit registers can be forwarded to the PCI Express device.

13.1.4 PCISTS—PCI Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 06h–07h
Attribute: R/WC, RO
Default Value: 0010h
Size: 16 bits

Bit	Description
15	**Detected Parity Error (DPE)** — R/WC. 0 = No parity error detected. 1 = Set when the root port receives a command or data from the backbone with a parity error. This is set even if PCIMD.PER (D28:F0/F1/F2/F3:04, bit 6) is not set.
14	**Signaled System Error (SSE)** — R/WC. 0 = No system error signaled. 1 = Set when the root port signals a system error to the internal SERR# logic.
13	**Received Master Abort (RMA)** — R/WC. 0 = Root port has not received a completion with unsupported request status from the backbone. 1 = Set when the root port receives a completion with unsupported request status from the backbone.
12	**Received Target Abort (RTA)** — R/WC. 0 = Root port has not received a completion with completer abort from the backbone. 1 = Set when the root port receives a completion with completer abort from the backbone.
11	**Signaled Target Abort (STA)** — R/WC. 0 = No target abort received. 1 = Set whenever the root port forwards a target abort received from the downstream device onto the backbone.
10:9	DEVSEL# Timing Status (DEV_STS) — Reserved per the *PCI Express* Base Specification*.
8	**Master Data Parity Error Detected (DPED)** — R/WC. 0 = No data parity error received. 1 = Set when the root port receives a completion with a data parity error on the backbone and PCIMD.PER (D28:F0/F1/F2/F3:04, bit 6) is set.
7	Fast Back to Back Capable (FB2BC) — Reserved per the *PCI Express* Base Specification*.
6	Reserved
5	66 MHz Capable — Reserved per the *PCI Express* Base Specification*.
4	**Capabilities List** — RO. Hardwired to 1. Indicates the presence of a capabilities list.
3	**Interrupt Status** — RO. Indicates status of Hot-Plug and power management interrupts on the root port that result in INTx# message generation. 0 = Interrupt is de-asserted. 1 = Interrupt is asserted. This bit is not set if MSI is enabled. If MSI is not enabled, this bit is set regardless of the state of PCICMD.Interrupt Disable bit (D28:F0/F1/F2/F3/F4/F5/F6/F7/F6/F7:04h:bit 10).
2:0	Reserved



13.1.5 RID—Revision Identification Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Offset Address: 08h Attribute: RO
Default Value: See bit description Size: 8 bits

Bit	Description
7:0	**Revision ID** — RO. This field indicates the device specific revision identifier.

13.1.6 PI—Programming Interface Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 09h Attribute: RO
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Programming Interface** — RO. 00h = No specific register level programming interface defined.

13.1.7 SCC—Sub Class Code Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 0Ah Attribute: RO
Default Value: 04h Size: 8 bits

Bit	Description
7:0	**Sub Class Code (SCC)** — RO. This field is determined by bit 2 of the MPC register (D28:F0-5:Offset D8h, bit 2). 04h = PCI-to-PCI bridge. 00h = Host Bridge.

13.1.8 BCC—Base Class Code Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 0Bh Attribute: RO
Default Value: 06h Size: 8 bits

Bit	Description
7:0	**Base Class Code (BCC)** — RO. 06h = Indicates the device is a bridge device.

13.1.9 CLS—Cache Line Size Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 0Ch Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Cache Line Size (CLS)** — R/W. This is read/write but contains no functionality, per the *PCI Express* Base Specification*.

13.1.10 PLT—Primary Latency Timer Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 0Dh
Attribute: RO
Default Value: 00h
Size: 8 bits

Bit	Description
7:3	Latency Count. Reserved per the *PCI Express* Base Specification.*
2:0	Reserved

13.1.11 HEADTYP—Header Type Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 0Eh
Attribute: RO
Default Value: 81h
Size: 8 bits

Bit	Description
7	**Multi-Function Device** — RO. 0 = Single-function device. 1 = Multi-function device.
6:0	**Configuration Layout**— RO. This field is determined by bit 2 of the MPC register (D28:F0-5:Offset D8h, bit 2). 00h = Indicates a Host Bridge. 01h = Indicates a PCI-to-PCI bridge.

13.1.12 BNUM—Bus Number Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

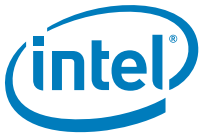
Address Offset: 18–1Ah
Attribute: R/W
Default Value: 000000h
Size: 24 bits

Bit	Description
23:16	**Subordinate Bus Number (SBBN)** — R/W. Indicates the highest PCI bus number below the bridge.
15:8	**Secondary Bus Number (SCBN)** — R/W. Indicates the bus number the port.
7:0	**Primary Bus Number (PBN)** — R/W. Indicates the bus number of the backbone.

13.1.13 SLT—Secondary Latency Timer Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 1Bh
Attribute: RO
Default Value: 00h
Size: 8 bits

Bit	Description
7:0	Secondary Latency Timer — Reserved for a Root Port per the *PCI Express* Base Specification.*



13.1.14 IOBL—I/O Base and Limit Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 1Ch–1Dh
Default Value: 0000h
Attribute: R/W, RO
Size: 16 bits

Bit	Description
15:12	**I/O Limit Address (IOLA)** — R/W. I/O Base bits corresponding to address lines 15:12 for 4-KB alignment. Bits 11:0 are assumed to be padded to FFFh.
11:8	**I/O Limit Address Capability (IOLC)** — RO. Indicates that the bridge does not support 32-bit I/O addressing.
7:4	**I/O Base Address (IOBA)** — R/W. I/O Base bits corresponding to address lines 15:12 for 4-KB alignment. Bits 11:0 are assumed to be padded to 000h.
3:0	**I/O Base Address Capability (IOBC)** — RO. Indicates that the bridge does not support 32-bit I/O addressing.

13.1.15 SSTS—Secondary Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 1Eh–1Fh
Default Value: 0000h
Attribute: R/WC
Size: 16 bits

Bit	Description
15	**Detected Parity Error (DPE)** — R/WC. 0 = No error. 1 = The port received a poisoned TLP.
14	**Received System Error (RSE)** — R/WC. 0 = No error. 1 = The port received an ERR_FATAL or ERR_NONFATAL message from the device.
13	**Received Master Abort (RMA)** — R/WC. 0 = Unsupported Request not received. 1 = The port received a completion with “Unsupported Request” status from the device.
12	**Received Target Abort (RTA)** — R/WC. 0 = Completion Abort not received. 1 = The port received a completion with “Completion Abort” status from the device.
11	**Signaled Target Abort (STA)** — R/WC. 0 = Completion Abort not sent. 1 = The port generated a completion with “Completion Abort” status to the device.
10:9	Secondary DEVSEL# Timing Status (SDTS): Reserved per *PCI Express* Base Specification*.
8	**Data Parity Error Detected (DPD)** — R/WC. 0 = Conditions below did not occur. 1 = Set when the BCTRL.PERE (D28:FO/F1/F2/F3/F4/F5:3E: bit 0) is set, and either of the following two conditions occurs: • Port receives completion marked poisoned. • Port poisons a write request to the secondary side.
7	Secondary Fast Back to Back Capable (SFBC): Reserved per *PCI Express* Base Specification*.
6	Reserved
5	Secondary 66 MHz Capable (SC66): Reserved per *PCI Express* Base Specification*.
4:0	Reserved

13.1.16 MBL—Memory Base and Limit Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset:	20h–23h	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits

Accesses that are within the ranges specified in this register will be sent to the attached device if CMD.MSE (D28:F0~F7:04:bit 1) is set. Accesses from the attached device that are outside the ranges specified will be forwarded to the backbone if CMD.BME (D28:F0~F7:04:bit 2) is set. The comparison performed is MB ≥ AD[31:20] ≤ ML.

Bit	Description
31:20	**Memory Limit (ML)** — R/W. These bits are compared with bits 31:20 of the incoming address to determine the upper 1-MB aligned value of the range.
19:16	Reserved
15:4	**Memory Base (MB)** — R/W. These bits are compared with bits 31:20 of the incoming address to determine the lower 1-MB aligned value of the range.
3:0	Reserved

13.1.17 PMBL—Prefetchable Memory Base and Limit Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset:	24h–27h	Attribute:	R/W, RO
Default Value:	00010001h	Size:	32 bits

Accesses that are within the ranges specified in this register will be sent to the device if CMD.MSE (D28:F0~F7;04, bit 1) is set. Accesses from the device that are outside the ranges specified will be forwarded to the backbone if CMD.BME (D28:F0~F7;04, bit 2) is set. The comparison performed is PMBU32:PMB ≥ AD[63:32]:AD[31:20] ≤ PMLU32:PML.

Bit	Description
31:20	**Prefetchable Memory Limit (PML)** — R/W. These bits are compared with bits 31:20 of the incoming address to determine the upper 1-MB aligned value of the range.
19:16	**64-bit Indicator (I64L)** — RO. Indicates support for 64-bit addressing
15:4	**Prefetchable Memory Base (PMB)** — R/W. These bits are compared with bits 31:20 of the incoming address to determine the lower 1-MB aligned value of the range.
3:0	**64-bit Indicator (I64B)** — RO. Indicates support for 64-bit addressing

13.1.18 PMBU32—Prefetchable Memory Base Upper 32 Bits Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset:	28h–2Bh	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits

Bit	Description
31:0	**Prefetchable Memory Base Upper Portion (PMBU)** — R/W. Upper 32-bits of the prefetchable address base.

13.1.19 PMLU32—Prefetchable Memory Limit Upper 32 Bits Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 2Ch–2Fh
Attribute: R/W
Default Value: 00000000h
Size: 32 bits

Bit	Description
31:0	**Prefetchable Memory Limit Upper Portion (PMLU)** — R/W. Upper 32-bits of the prefetchable address limit.

13.1.20 CAPP—Capabilities List Pointer Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 34h
Attribute: RWO
Default Value: 40h
Size: 8 bits

Bit	Description
7:0	**Capabilities Pointer (PTR)** — RO. Indicates that the pointer for the first entry in the capabilities list is at 40h in configuration space.

13.1.21 INTR—Interrupt Information Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 3Ch–3Dh
Attribute: R/W, RO
Default Value: See bit description
Size: 16 bits
Function Level Reset: No (Bits 7:0 only)

Bit	Description
15:8	**Interrupt Pin (IPIN)** — RO. Indicates the interrupt pin driven by the root port. At reset, this register takes on the following values that reflect the reset state of the D28IP register in chipset config space: Port — Reset Value 1 — D28IP.P1IP 2 — D28IP.P2IP 3 — D28IP.P3IP 4 — D28IP.P4IP 5 — D28IP.P5IP 6 — D28IP.P6IP 7 — D28IP.P7IP 8 — D28IP.P8IP ***Note:*** The value that is programmed into D28IP is always reflected in this register.
7:0	**Interrupt Line (ILINE)** — R/W. Default = 00h. Software written value to indicate which interrupt line (vector) the interrupt is connected to. No hardware action is taken on this register. These bits are not reset by FLR.

13.1.22 BCTRL—Bridge Control Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 3Eh–3Fh
Attribute: R/W
Default Value: 0000h
Size: 16 bits

Bit	Description
15:12	Reserved
11	**Discard Timer SERR# Enable (DTSE):** Reserved per *PCI Express* Base Specification,* Rev. 1.0a
10	**Discard Timer Status (DTS):** Reserved per *PCI Express* Base Specification,* Revision 1.0a.
9	**Secondary Discard Timer (SDT):** Reserved per *PCI Express* Base Specification,* Revision 1.0a.
8	**Primary Discard Timer (PDT):** Reserved per *PCI Express* Base Specification,* Revision 1.0a.
7	**Fast Back to Back Enable (FBE):** Reserved per *PCI Express* Base Specification,* Revision 1.0a.
6	**Secondary Bus Reset (SBR)** — R/W. Triggers a hot reset on the PCI Express* port.
5	**Master Abort Mode (MAM):** Reserved per Express specification.
4	**VGA 16-Bit Decode (V16)** — R/W. 0 = VGA range is enabled. 1 = The I/O aliases of the VGA range (see BCTRL:VE definition below), are not enabled, and only the base I/O ranges can be decoded.
3	**VGA Enable (VE)**— R/W. 0 = The ranges below will not be claimed off the backbone by the root port. 1 = The following ranges will be claimed off the backbone by the root port: • Memory ranges A0000h-BFFFFh • I/O ranges 3B0h – 3BBh and 3C0h – 3DFh, and all aliases of bits 15:10 in any combination of 1s
2	**ISA Enable (IE)** — R/W. This bit only applies to I/O addresses that are enabled by the I/O Base and I/O Limit registers and are in the first 64 KB of PCI I/O space. 0 = The root port will not block any forwarding from the backbone as described below. 1 = The root port will block any forwarding from the backbone to the device of I/O transactions addressing the last 768 bytes in each 1-KB block (offsets 100h to 3FFh).
1	**SERR# Enable (SE)** — R/W. 0 = The messages described below are not forwarded to the backbone. 1 = ERR_COR, ERR_NONFATAL, and ERR_FATAL messages received are forwarded to the backbone.
0	**Parity Error Response Enable (PERE)** — R/W. When set, 0 = Poisoned write TLPs and completions indicating poisoned TLPs will not set the SSTS.DPD (D28:F0/F1/F2/F3/F4/F5/F6/F7:1E, bit 8). 1 = Poisoned write TLPs and completions indicating poisoned TLPs will set the SSTS.DPD (D28:F0/F1/F2/F3/F4/F5/F6/F7:1E, bit 8).

13.1.23 CLIST—Capabilities List Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 40–41h
Attribute: R/WO, RO
Default Value: 8010h
Size: 16 bits

Bit	Description
15:8	**Next Capability (NEXT)** — RWO. Indicates the location of the next pointer. The default value of this register is 80h, which points to the MSI Capability structure. Since this is a RWO register, BIOS must write a value to this register, even if it is to re-write the default value.
7:0	**Capability ID (CID)** — RO. Indicates this is a PCI Express* capability.

13.1.24 XCAP—PCI Express* Capabilities Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 42h–43h
Default Value: 0042h
Attribute: R/WO, RO
Size: 16 bits

Bit	Description
15:14	Reserved
13:9	**Interrupt Message Number (IMN)** — RO. Intel® Xeon® Processor D-1500 Product Family does not have multiple MSI interrupt numbers.
8	**Slot Implemented (SI)** — R/WO. Indicates whether the root port is connected to a slot. Slot support is platform specific. BIOS programs this field, and it is maintained until a platform reset.
7:4	**Device / Port Type (DT)** — RO. Indicates this is a PCI Express* root port.
3:0	**Capability Version (CV)** — RO. Indicates PCI Express 2.0.

13.1.25 DCAP—Device Capabilities Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 44h–47h
Default Value: 00008000h
Attribute: R/WO, RO
Size: 32 bits

Bit	Description
31:28	Reserved
27:26	**Captured Slot Power Limit Scale (CSPS)** — RO. Not supported.
25:18	**Captured Slot Power Limit Value (CSPV)** — RO. Not supported.
17:16	Reserved
15	**Role Based Error Reporting (RBER)** — RO. Indicates that this device implements the functionality defined in the Error Reporting ECN as required by the PCI Express 2.0 specification.
14:12	Reserved
11:9	**Endpoint L1 Acceptable Latency (E1AL)** — RO. This field is reserved with a setting of 000b for devices other than Endpoints, per the PCI Express 2.0 Spec.
8:6	**Endpoint L0 Acceptable Latency (E0AL)** — RO. This field is reserved with a setting of 000b for devices other than Endpoints, per the PCI Express 2.0 Spec.
5	**Extended Tag Field Supported (ETFS)** — RO. Indicates that 8-bit tag fields are supported.
4:3	**Phantom Functions Supported (PFS)** — RO. No phantom functions supported.
2:0	**Max Payload Size Supported (MPS)** — RWO. BIOS should write to this field during system initialization. Only a maximum payload size of 128B is supported. Programming this field to any value other than 000b (128B) will result in aliasing to 128B max payload size.

13.1.26 DCTL—Device Control Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 48h–49h
Default Value: 0000h
Attribute: R/W, RO
Size: 16 bits

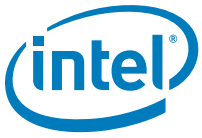
Bit	Description
15	Reserved
14:12	**Max Read Request Size (MRRS)** — RO. Hardwired to 0.
11	**Enable No Snoop (ENS)** — RO. Not supported. The root port will never issue non-snoop requests.
10	**Aux Power PM Enable (APME)** — R/W. The OS will set this bit to 1 if the device connected has detected aux power. It has no effect on the root port otherwise.
9	**Phantom Functions Enable (PFE)** — RO. Not supported.
8	**Extended Tag Field Enable (ETFE)** — RO. Not supported.

Bit	Description
7:5	**Max Payload Size (MPS)** — R/W. The root port only supports 128B max payloads, regardless of the programming of this field. Programming this field to any value other than 000b (128B) will result in aliasing to 128B max payload size. BIOS should program this field prior to enabling BME.
4	**Enable Relaxed Ordering (ERO)** — RO. Not supported.
3	**Unsupported Request Reporting Enable (URE)** — R/W. 0 = The root port will ignore unsupported request errors. 1 = Allows signaling ERR_NONFATAL, ERR_FATAL, or ERR_COR to the Root Control register when detecting an unmasked Unsupported Request (UR). An ERR_COR is signaled when a unmasked Advisory Non-Fatal UR is received. An ERR_FATAL, ERR_or NONFATAL, is sent to the Root Control Register when an uncorrectable non-Advisory UR is received with the severity set by the Uncorrectable Error Severity register.
2	**Fatal Error Reporting Enable (FEE)** — R/W. 0 = The root port will ignore fatal errors. 1 = Enables signaling of ERR_FATAL to the Root Control register due to internally detected errors or error messages received across the link. Other bits also control the full scope of related error reporting.
1	**Non-Fatal Error Reporting Enable (NFE)** — R/W. 0 = The root port will ignore non-fatal errors. 1 = Enables signaling of ERR_NONFATAL to the Root Control register due to internally detected errors or error messages received across the link. Other bits also control the full scope of related error reporting.
0	**Correctable Error Reporting Enable (CEE)** — R/W. 0 = The root port will ignore correctable errors. 1 = Enables signaling of ERR_CORR to the Root Control register due to internally detected errors or error messages received across the link. Other bits also control the full scope of related error reporting.

13.1.27 DSTS—Device Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 4Ah–4Bh
Attribute: R/WC, RO
Default Value: 0010h
Size: 16 bits

Bit	Description
15:6	Reserved
5	**Transactions Pending (TDP)** — RO. This bit has no meaning for the root port since only one transaction may be pending to Intel® Xeon® Processor D-1500 Product Family, so a read of this bit cannot occur until it has already returned to 0.
4	**AUX Power Detected (APD)** — RO. The root port contains AUX power for wakeup.
3	**Unsupported Request Detected (URD)** — R/WC. Indicates an unsupported request was detected.
2	**Fatal Error Detected (FED)** — R/WC. Indicates a fatal error was detected. 0 = Fatal has not occurred. 1 = A fatal error occurred from a data link protocol error, link training error, buffer overflow, or malformed TLP.
1	**Non-Fatal Error Detected (NFED)** — R/WC. Indicates a non-fatal error was detected. 0 = Non-fatal has not occurred. 1 = A non-fatal error occurred from a poisoned TLP, unexpected completions, unsupported requests, completer abort, or completer timeout.
0	**Correctable Error Detected (CED)** — R/WC. Indicates a correctable error was detected. 0 = Correctable has not occurred. 1 = The port received an internal correctable error from receiver errors / framing errors, TLP CRC error, DLLP CRC error, replay num rollover, replay timeout.



13.1.28 LCAP—Link Capabilities Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 4Ch–4Fh
Attribute: R/WO, RO/V, RO
Default Value: See bit description
Size: 32 bits

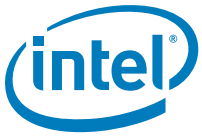
Bit	Description
31:24	**Port Number (PN)** — RO/V. Indicates the port number for the root port. This value is different for each implemented port: **Function** / **Port #** / **Value of PN Field** D28:F0 / 1 / 01h D28:F1 / 2 / 02h D28:F2 / 3 / 03h D28:F3 / 4 / 04h D28:F4 / 5 / 05h D28:F5 / 6 / 06h D28:F6 / 7 / 07h D28:F7 / 8 / 08h
23:22	Reserved
21	**Link Bandwidth Notification Capability (LBNC)** — RO. Hardwired to 1b to indicate that this port supports Link Bandwidth Notification status and interrupt mechanisms.
20	**Link Active Reporting Capable (LARC)** — RO. Hardwired to 1b to indicate that this port supports the optional capability of reporting the DL_Active state of the Data Link Control and Management State Machine.
19	Reserved
18	**Clock Power Management (CPM)** — RO. 0 = Intel® Xeon® Processor D-1500 Product Family root ports do not support the CLKREQ# mechanism. 1 = Intel® Xeon® Processor D-1500 Product Family root ports support the CLKREQ# mechanism.
17:15	**L1 Exit Latency (EL1)** — R/WO. Indicates an exit latency of 2us to 4us. 000b = Less than 1us 001b = 1 us to less than 2 us 010b = 2 us to less than 4 us 011b = 4 us to less than 8 us 100b = 8 us to less than 16 us 101b = 16 us to less than 32 us 110b = 32 us to 64 us 111b = more than 64 us ***Note:*** If PXP PLL shutdown is enabled, BIOS should program this latency to comprehend PLL lock latency.
14:12	**L0s Exit Latency (EL0)** — RO/V. Indicates an exit latency based upon common-clock configuration. **LCLT.CCC** / **Value of EL0 (these bits)** 0 / MPC.UCEL (D28:F0~F7:D8h:bits20:18) 1 / MPC.CCEL (D28:F0~F7:D8h:bits17:15) ***Note:*** LCLT.CCC is at D28:F0~F7:50h:bit 6.

Bit	Description
11:10	**Active State Power Management Support (APMS)** — R/WO. Indicates what level of active state link power management is supported on the root port. **Value** — **Definition** 00b — Reserved 01b — L0s Entry Supported 10b — Reserved 11b — Both L0s and L1 Entry Supported
9:4	**Maximum Link Width (MLW)** — RO/V. These bits are set by the PCIEPCS1[1:0] soft strap in the PCHSTRP9 record. ***Note:*** Support for 1 x2 or 1 x4 configuration on PCIe Port 1 is only available per Section 3.1 guidelines. 000011 = 1 x4: Port 1 (x4) 000010 = Reserved 000001 = 1 x2 and 2 x1s: Port 1 (x2), Port 3 (x1) and Port 4 (x1) 000000 = 4 x1s: Port 1 (x1), Port 2 (x1), Port 3 (x1) and Port 4 (x1) This bit is set by the PCIEPCS2[1:0] soft strap in the PCHSTRP9 record. 000011 = 1 x4: Port 5 (x4) 000010 = Reserved 000001 = 1 x2 and 2 x1s: Port 5 (x2), Port 7 (x1) and Port 8 (x1) 000000 = 4 x1s: Port 5 (x1), Port 6 (x1), Port 7 (x1) and Port 8 (x1)
3:0	**Maximum Link Speed (MLS)** — RO. 0001b = indicates the link speed is 2.5 Gb/s 0010b = 5.0 Gb/s and 2.5Gb/s link speeds supported ***Note:*** These bits report a value of 0001b if Gen2 disable bit 14 is set in the MPC register, else the value reported is 0010b

13.1.29 LCTL—Link Control Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 50h–51h — Attribute: R/W, RO
Default Value: 0000h — Size: 16 bits

Bit	Description
15:10	Reserved
9	**Hardware Autonomous Width Disable** – RO. Hardware never attempts to change the link width except when attempting to correct unreliable Link operation.
8	Reserved
7	**Extended Synch (ES)** — R/W. 0 = Extended synch disabled. 1 = Forces extended transmission of FTS ordered sets in FTS and extra TS2 at exit from L1 prior to entering L0.
6	**Common Clock Configuration (CCC)** — R/W. 0 = Intel® Xeon® Processor D-1500 Product Family and device are not using a common reference clock. 1 = Intel® Xeon® Processor D-1500 Product Family and device are operating with a distributed common reference clock.



Bit	Description
5	**Retrain Link (RL)** — R/W. 0 = This bit always returns 0 when read. 1 = The root port will train its downstream link. ***Note:*** Software uses LSTS.LT (D28:F0/F1/F2/F3/F4/F5/F6/F7:52, bit 11) to check the status of training. ***Note:*** It is permitted to write 1b to this bit while simultaneously writing modified values to other fields in this register. If the LTSSM is not already in Recovery or Configuration, the resulting Link training must use the modified values. If the LTSSM is already in Recovery or Configuration, the modified values are not required to affect the Link training that is already in progress.
4	**Link Disable (LD)** — R/W. 0 = Link enabled. 1 = The root port will disable the link.
3	**Read Completion Boundary Control (RCBC)** — RO. Indicates the read completion boundary is 64 bytes.
2	Reserved
1:0	**Active State Link PM Control (APMC)** — R/W. Indicates whether the root port should enter L0s or L1 or both. 00 = Disabled 01 = L0s Entry Enabled 10 = L1 Entry Enabled 11 = L0s and L1 Entry Enabled

13.1.30 LSTS—Link Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 52h–53h
Attribute: RO
Default Value: See bit description
Size: 16 bits

Bit	Description
15:14	Reserved
13	**Data Link Layer Active (DLLA)** — RO. Default value is 0b. 0 = Data Link Control and Management State Machine is not in the DL_Active state 1 = Data Link Control and Management State Machine is in the DL_Active state
12	**Slot Clock Configuration (SCC)** — RO. Set to 1b to indicate that Intel® Xeon® Processor D-1500 Product Family uses the same reference clock as on the platform and does not generate its own clock.
11	**Link Training (LT)** — RO. Default value is 0b. 0 = Link training completed. 1 = Link training is occurring.
10	**Link Training Error (LTE)** — RO. Not supported. Set value is 0b.
9:4	**Negotiated Link Width (NLW)** — RO. This field indicates the negotiated width of the given PCI Express* link. The contents of this NLW field is undefined if the link has not successfully trained. **Port # — Possible Values** 1 — 000001b, 000010b, 000100b 2 — 000001b 3 — 000001b, 000010b 4 — 000001b 5 — 000001b, 000010b, 000100b 6 — 000001b 7 — 000001b, 000010b 8 — 000001b ***Note:*** 000001b = x1 link width, 000010b =x2 linkwidth, 000100b = x4 linkwidth

Bit	Description
3:0	**Link Speed (LS)** — RO. This field indicates the negotiated Link speed of the given PCI Express* link. 0001b = Link is 2.5 Gb/s 0010b = Link is 5.0 Gb/s

13.1.31 SLCAP—Slot Capabilities Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 54h–57h Attribute: R/WO, RO
Default Value: 00060060h Size: 32 bits

Bit	Description
31:19	**Physical Slot Number (PSN)** — R/WO. This is a value that is unique to the slot number. BIOS sets this field and it remains set until a platform reset.
18:17	Reserved
16:15	**Slot Power Limit Scale (SLS)** — R/WO. Specifies the scale used for the slot power limit value. BIOS sets this field and it remains set until a platform reset.
14:7	**Slot Power Limit Value (SLV)** — R/WO. Specifies the upper limit (in conjunction with SLS value), on the upper limit on power supplied by the slot. The two values together indicate the amount of power in watts allowed for the slot. BIOS sets this field and it remains set until a platform reset.
6	**Hot-Plug Capable (HPC)** — R/WO. 1b = Indicates that Hot-Plug is supported.
5	**Hot-Plug Surprise (HPS)** — R/WO. 1b = Indicates the device may be removed from the slot without prior notification.
4	**Power Indicator Present (PIP)** — RO. 0b = Indicates that a power indicator LED is not present for this slot.
3	**Attention Indicator Present (AIP)** — RO. 0b = Indicates that an attention indicator LED is not present for this slot.
2	**MRL Sensor Present (MSP)** — RO. 0b = Indicates that an MRL sensor is not present.
1	**Power Controller Present (PCP)** — RO. 0b = Indicates that a power controller is not implemented for this slot.
0	**Attention Button Present (ABP)** — RO. 0b = Indicates that an attention button is not implemented for this slot.

13.1.32 SLCTL—Slot Control Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 58h–59h Attribute: R/W, RO
Default Value: 0000h Size: 16 bits

Bit	Description
15:13	Reserved
12	**Link Active Changed Enable (LACE)** — R/W. When set, this field enables generation of a Hot-Plug interrupt when the Data Link Layer Link Active field (D28:F0/F1/F2/F3/F4/F5/F6/F7:52h:bit 13) is changed.
11	Reserved
10	**Power Controller Control (PCC)** — RO.This bit has no meaning for module based Hot-Plug.
9:6	Reserved
5	**Hot-Plug Interrupt Enable (HPE)** — R/W. 0 = Hot-Plug interrupts based on Hot-Plug events is disabled. 1 = Enables generation of a Hot-Plug interrupt on enabled Hot-Plug events.
4	Reserved

Bit	Description
3	**Presence Detect Changed Enable (PDE)** — R/W. 0 = Hot-Plug interrupts based on presence detect logic changes is disabled. 1 = Enables the generation of a Hot-Plug interrupt or wake message when the presence detect logic changes state.
2:0	Reserved

13.1.33 SLSTS—Slot Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 5Ah–5Bh
Attribute: R/WC, RO
Default Value: 0000h
Size: 16 bits

Bit	Description
15:9	Reserved
8	**Link Active State Changed (LASC)** — R/WC. 1 = This bit is set when the value reported in Data Link Layer Link Active field of the Link Status register (D28:F0/F1/F2/F3/F4/F5/F6/F7:52h:bit 13) is changed. In response to a Data Link Layer State Changed event, software must read Data Link Layer Link Active field of the Link Status register to determine if the link is active before initiating configuration cycles to the hot plugged device.
7	Reserved
6	**Presence Detect State (PDS)** — RO. If XCAP.SI (D28:F0/F1/F2/F3/F4/F5/F6/F7:42h:bit 8) is set (indicating that this root port spawns a slot), then this bit: 0 = Indicates the slot is empty. 1 = Indicates the slot has a device connected. Otherwise, if XCAP.SI is cleared, this bit is always set (1).
5	**MRL Sensor State (MS)** — Reserved as the MRL sensor is not implemented.
4	Reserved
3	**Presence Detect Changed (PDC)** — R/WC. 0 = No change in the PDS bit. 1 = The PDS bit changed states.
2	**MRL Sensor Changed (MSC)** — Reserved as the MRL sensor is not implemented.
1	**Power Fault Detected (PFD)** — Reserved as a power controller is not implemented.
0	Reserved

13.1.34 RCTL—Root Control Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 5Ch–5Dh
Attribute: R/W
Default Value: 0000h
Size: 16 bits

Bit	Description
15:4	Reserved
3	**PME Interrupt Enable (PIE)** — R/W. 0 = Interrupt generation disabled. 1 = Interrupt generation enabled when PCISTS.Inerrupt Status (D28:F0~F7:60h, bit 16) is in a set state (either due to a 0 to 1 transition, or due to this bit being set with RSTS.IS already set).
2	**System Error on Fatal Error Enable (SFE)** — R/W. 0 = An SERR# will not be generated. 1 = An SERR# will be generated, assuming CMD.SEE (D28:F0~F7:04, bit 8) is set, if a fatal error is reported by any of the devices in the hierarchy of this root port, including fatal errors in this root port.

Bit	Description
1	**System Error on Non-Fatal Error Enable (SNE)** — R/W. 0 = An SERR# will not be generated. 1 = An SERR# will be generated, assuming CMD.SEE (D28:F0~F7:04, bit 8) is set, if a non-fatal error is reported by any of the devices in the hierarchy of this root port, including non-fatal errors in this root port.
0	**System Error on Correctable Error Enable (SCE)** — R/W. 0 = An SERR# will not be generated. 1 = An SERR# will be generated, assuming CMD.SEE (D28:F0~F7:04, bit 8) if a correctable error is reported by any of the devices in the hierarchy of this root port, including correctable errors in this root port.

13.1.35 RSTS—Root Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

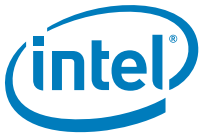
Address Offset: 60h–63h Attribute: R/WC, RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:18	Reserved
17	**PME Pending (PP)** — RO. 0 = When the original PME is cleared by software, it will be set again, the requestor ID will be updated, and this bit will be cleared. 1 = Indicates another PME is pending when the PME status bit is set.
16	**PME Status (PS)** — R/WC. 0 = PME was not asserted. 1 = Indicates that PME was asserted by the requestor ID in RID. Subsequent PMEs are kept pending until this bit is cleared.
15:0	**PME Requestor ID (RID)** — RO. Indicates the PCI requestor ID of the last PME requestor. Valid only when PS is set.

13.1.36 DCAP2—Device Capabilities 2 Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 64h–67h Attribute: RWO, RO
Default Value: 00080816h Size: 32 bits

Bit	Description
31:12	Reserved
11	**LTR Mechanism Supported (LTRMS)** — RWO. A value of 1b indicates support for the optional Latency Tolerance Reporting (LTR) mechanism.
10:5	Reserved
4	**Completion Timeout Disable Supported (CTDS)** — RO. A value of 1b indicates support for the Completion Timeout Disable mechanism.
3:0	**Completion Timeout Ranges Supported (CTRS) –** RO. This field indicates device support for the optional Completion Timeout programmability mechanism. This mechanism allows system software to modify the Completion Timeout value. This field is hardwired to support 10 ms to 250 ms and 250 ms to 4 s.



13.1.37 DCTL2—Device Control 2 Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 68h–69h
Attribute: RO, R/W
Default Value: 0000h
Size: 16 bits

Bit	Description
15:11	Reserved
10	**LTR Mechanism Enable (LTREN)** — RW. A value of 1b enables support for the optional Latency Tolerance Reporting (LTR) mechanism.
9:5	Reserved
4	**Completion Timeout Disable (CTD)** — R/W. When set to 1b, this bit disables the Completion Timeout mechanism. If there are outstanding requests when the bit is cleared, it is permitted but not required for hardware to apply the completion timeout mechanism to the outstanding requests. If this is done, it is permitted to base the start time for each request on either the time this bit was cleared or the time each request was issued.
3:0	**Completion Timeout Value (CTV)** — R/W. In Devices that support Completion Timeout programmability, this field allows system software to modify the Completion Timeout value. This field is applicable to Root Ports, Endpoints that issue requests on their own behalf, and PCI Express* to PCI/PCI-X Bridges that take ownership of requests issued on PCI Express. For all other devices this field is reserved and must be hardwired to 0000b. A Device that does not support this optional capability must hardwire this field to 0000b and is required to implement a timeout value in the range 50 us to 50 ms. Devices that support Completion Timeout programmability must support the values given below, corresponding to the programmability ranges indicated in the Completion Timeout Values Supported field. Intel® Xeon® Processor D-1500 Product Family targeted configurable ranges are listed below, along with the range allowed by the PCI Express 2.0 specification. Defined encodings: 0000b = Default range: 40 ms to 50 ms (specification range 50 us to 50 ms) Values available if Range A (50 us to 10 ms) programmability range is supported: 0001b = 90 µs to 100 µs (specification range is 50 µs to 100 µs) 0010b = 9 ms to 10ms (specification range is 1 ms to 10 ms) Values available if Range B (10 ms to 250 ms) programmability range is supported: 0101b = 40 ms to 50 ms (specification range is 16 ms to 55 ms) 0110b = 160 ms to 170 ms (specification range is 65 ms to 210 ms) Values available if Range C (250 ms to 4s) programmability range is supported: 1001b = 400 ms to 500 ms (specification range is 260 ms to 900 ms) 1010b = 1.6s to 1.7s (specification range is 1s to 3.5s) All other values are Reserved. ***Note:*** Software is permitted to change the value in this field at any time. For requests already pending when the Completion Timeout Value is changed, hardware is permitted to use either the new or the old value for the outstanding requests, and is permitted to base the start time for each request either on when this value was changed or on when each request was issued.

13.1.38 LCTL2—Link Control 2 Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 70h–71h
Attribute: R/W
Default Value: 0002h
Size: 16 bits

Bit	Description
15:13	Reserved
12	**Compliance De-Emphasis (CD) —** R/W. This bit sets the de-emphasis level in Polling.Compliance state if the entry occurred due to the Enter Compliance bit being 1b. Encodings: 0 = -6 dB 1 = -3.5 dB When the Link is operating at 2.5 GT/s, the setting of this bit has no effect. The default value of this bit is 0b. This bit is intended for debug, compliance testing purposes. System firmware and software are allowed to modify this bit only during debug or compliance testing.
11	**Compliance SOS (CSOS) —** R/W. When set to 1b, the LTSSM is required to send SKP Ordered Sets periodically in between the (modified) compliance patterns. The default value of this bit is 0b.
10	**Enter Modified Compliance (EMC) —** R/W. When this bit is set to 1b, the device transmits Modified Compliance Pattern if the LTSSM enters Polling.Compliance substrate. This register is intended for debug, compliance testing purposes only and the system must ensure it is set to the default value during normal operation. The default value of this bit is 0b.
9:7	**Transmit Margin (TM) —** R/W. This field controls the value of the non-de-emphasized voltage level at the Transmitter pins. This field is reset to 000b on entry to the LTSSM Polling.Configuration substrate (see PCI Express Chapter 4 for details of how the Transmitter voltage level is determined in various states). **Encodings:** 000b: Normal operating range 001b: 800-1200 mV for full swing and 400-700 mV for half-swing 010b - (n-1): Values must be monotonic with a non-zero slope. The value of n must be greater than 3 and less than 7. At least two of these must be below the normal operating range of n: 200–400 mV for full-swing and 100–200 mV for half-swing n - 111b” Reserved For a Multi-Function device associated with an Upstream Port, the field in Function 0 is of type RWS, and only Function 0 controls the component‘s Link behavior. In all other Functions of that device, this field is of type RsvdP. Default value of this field is 000b. Components that support only the 2.5 GT/s speed are permitted to hardwire this bit to 000b. This register is intended for debug, compliance testing purposes only and the system must ensure it is set to the default value during normal operation.
6	**Selectable De-emphasis (SD) —** R/W. When the Link is operating at 5.0 GT/s speed, this bit selects the level of de-emphasis for an Upstream component. Encodings: 1b -3.5 dB 0b -6 dB When the Link is operating at 2.5 GT/s speed, the setting of this bit has no effect.
5	Reserved
4	**Enter Compliance (EC) —** R/W. Software is permitted to force a Link to enter Compliance mode at the speed indicated in the Target Link Speed field by setting this bit to 1b in both components on a Link and then initiating a hot reset on the Link.
3:0	**Target Link Speed (TLS)**— R/W. This field sets an upper limit on Link operational speed by restricting the values advertised by the upstream component in its training sequences. 0001b = 2.5 GT/s Target Link Speed 0010b = 5.0 GT/s and 2.5 GT/s Target Link Speeds All other values reserved.

13.1.39 LSTS2—Link Status 2 Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 72h–73h
Default Value: 0000h
Attribute: RO
Size: 16 bits

Bit	Description
15:1	Reserved
0	**Current De-emphasis Level (CDL)** — RO. When the Link is operating at 5 GT/s speed, this bit reflects the level of de-emphasis. Encodings: 0 = -6 dB 1 = -3.5 dB The value in this bit is undefined when the Link is operating at 2.5 GT/s speed.

13.1.40 MID—Message Signaled Interrupt Identifiers Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 80h–81h
Default Value: 9005h
Attribute: RO
Size: 16 bits

Bit	Description
15:8	**Next Pointer (NEXT)** — RO. Indicates the location of the next pointer in the list.
7:0	**Capability ID (CID)** — RO. Capabilities ID indicates MSI.

13.1.41 MC—Message Signaled Interrupt Message Control Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 82–83h
Default Value: 0000h
Attribute: R/W, RO
Size: 16 bits

Bit	Description
15:8	Reserved
7	**64 Bit Address Capable (C64)** — RO. Capable of generating a 32-bit message only.
6:4	**Multiple Message Enable (MME)** — R/W. These bits are R/W for software compatibility, but only one message is ever sent by the root port.
3:1	**Multiple Message Capable (MMC)** — RO. Only one message is required.
0	**MSI Enable (MSIE)** — R/W. 0 = MSI is disabled. 1 = MSI is enabled and traditional interrupt pins are not used to generate interrupts. ***Note:*** CMD.BME (D28:F0/F1/F2/F3/F4/F5/F6/F7:04h:bit 2) must be set for an MSI to be generated. If CMD.BME is cleared, and this bit is set, no interrupts (not even pin based) are generated.

13.1.42 MA—Message Signaled Interrupt Message Address Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 84h–87h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits

Bit	Description
31:2	**Address (ADDR)** — R/W. Lower 32 bits of the system specified message address, always DW aligned.
1:0	Reserved

13.1.43 MD—Message Signaled Interrupt Message Data Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 88h–89h
Attribute: R/W
Default Value: 0000h
Size: 16 bits

Bit	Description
15:0	**Data (DATA)** — R/W. This 16-bit field is programmed by system software if MSI is enabled. Its content is driven onto the lower word (PCI AD[15:0]) during the data phase of the MSI memory write transaction.

13.1.44 SVCAP—Subsystem Vendor Capability Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 90h–91h
Attribute: R/WO, RO
Default Value: A00Dh
Size: 16 bits

Bit	Description
15:8	**Next Capability (NEXT)** — R/WO. Indicates the location of the next pointer in the list. As this register is RWO, BIOS must write a value to this register, even if it is to re-write the default value.
7:0	**Capability Identifier (CID)** — RO. Value of 0Dh indicates this is a PCI bridge subsystem vendor capability.

13.1.45 SVID—Subsystem Vendor Identification Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 94h–97h
Attribute: R/WO
Default Value: 00000000h
Size: 32 bits

Bit	Description
31:16	**Subsystem Identifier (SID)** — R/WO. Indicates the subsystem as identified by the vendor. This field is write once and is locked down until a bridge reset occurs (not the PCI bus reset).
15:0	**Subsystem Vendor Identifier (SVID)** — R/WO. Indicates the manufacturer of the subsystem. This field is write once and is locked down until a bridge reset occurs (not the PCI bus reset).

13.1.46 PMCAP—Power Management Capability Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: A0h–A1h
Attribute: RO
Default Value: 0001h
Size: 16 bits

Bit	Description
15:8	**Next Capability (NEXT)** — RO. Indicates this is the last item in the list.
7:0	**Capability Identifier (CID)** — RO. Value of 01h indicates this is a PCI power management capability.

13.1.47 PMC—PCI Power Management Capabilities Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: A2h–A3h
Attribute: RO
Default Value: C803h
Size: 16 bits

Bit	Description
15:11	**PME_Support (PMES)** — RO. Indicates PME# is supported for states D0, $D3_{HOT}$ and $D3_{COLD}$. The root port does not generate PME#, but reporting that it does is necessary for some legacy operating systems to enable PME# in devices connected behind this root port.
10	D2_Support (D2S) — RO. The D2 state is not supported.
9	D1_Support (D1S) — RO The D1 state is not supported.
8:6	**Aux_Current (AC)** — RO. Reports 375 mA maximum suspend well current required when in the $D3_{COLD}$ state.
5	**Device Specific Initialization (DSI)** — RO. 1 = Indicates that no device-specific initialization is required.
4	Reserved
3	**PME Clock (PMEC)** — RO. 1 = Indicates that PCI clock is not required to generate PME#.
2:0	**Version (VS)** — RO. Indicates support for *Revision 1.2 of the PCI Power Management Specification*.

13.1.48 PMCS—PCI Power Management Control and Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: A4h–A7h
Attribute: R/W, RO
Default Value: 00000000h
Size: 32 bits

Bit	Description
31:24	Reserved
23	Bus Power / Clock Control Enable (BPCE) — Reserved per *PCI Express* Base Specification, Revision 1.0a*.
22	B2/B3 Support (B23S) — Reserved per *PCI Express* Base Specification, Revision 1.0a*.
21:16	Reserved
15	**PME Status (PMES)** — RO. 1 = Indicates a PME was received on the downstream link.
14:9	Reserved
8	**PME Enable (PMEE)** — R/W. 1 = Indicates PME is enabled. The root port takes no action on this bit, but it must be R/W for some legacy operating systems to enable PME# on devices connected to this root port. This bit is sticky and resides in the resume well. The reset for this bit is RSMRST# which is not asserted during a warm reset.
7:2	Reserved
1:0	**Power State (PS)** — R/W. This field is used both to determine the current power state of the root port and to set a new power state. The values are: 00 = D0 state 11 = $D3_{HOT}$ state ***Note:*** When in the $D3_{HOT}$ state, the controller's configuration space is available, but the I/O and memory spaces are not. Type 1 configuration cycles are also not accepted. Interrupts are not required to be blocked as software will disable interrupts prior to placing the port into D3HOT. If software attempts to write a '10' or '01' to these bits, the write will be ignored.

13.1.49 MPC2—Miscellaneous Port Configuration Register 2 (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

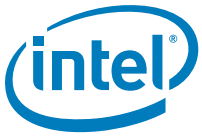
Address Offset: D4h–D7h
Attribute: R/W, RO
Default Value: 00000800h
Size: 32 bits

Bit	Description
31:5	Reserved
4	ASPM Control Override Enable (ASPMCOEN) — R/W. 1 = Root port will use the values in the ASPM Control Override registers 0 = Root port will use the ASPM Registers in the Link Control register. ***Notes:*** This register allows BIOS to control the root port ASPM settings instead of the OS.
3:2	**ASPM Control Override (ASPMO)** — R/W. Provides BIOS control of whether root port should enter L0s or L1 or both. 00 = Disabled 01 = L0s Entry Enabled 10 = L1 Entry Enabled 11 = L0s and L1 Entry Enabled.
1	**EOI Forwarding Disable (EOIFD)** — R/W. When set, EOI messages are not claimed on the backbone by this port an will not be forwarded across the PCIe link. 0 = Broadcast EOI messages that are sent on the backbone are claimed by this port and forwarded across the PCIe* link. 1 = Broadcast EOI messages are not claimed on the backbone by this port and will not be forwarded across the PCIe Link.
0	**L1 Completion Timeout Mode (LICTM)** — R/W. 0 = PCI Express Specification Compliant. Completion timeout is disabled during software initiated L1, and enabled during ASPM initiate L1. 1 = Completion timeout is enabled during L1, regardless of how L1 entry was initiated.

13.1.50 MPC—Miscellaneous Port Configuration Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: D8h–dBh
Attribute: R/W, RO, R/WO
Default Value: 09110000h
Size: 32 bits

Bit	Description
31	**Power Management SCI Enable (PMCE)** — R/W. 0 = SCI generation based on a power management event is disabled. 1 = Enables the root port to generate SCI whenever a power management event is detected.
30	**Hot-Plug SCI Enable (HPCE)** — R/W. 0 = SCI generation based on a Hot-Plug event is disabled. 1 = Enables the root port to generate SCI whenever a Hot-Plug event is detected.
29	Link Hold Off (LHO) — R/W. 1 = Port will not take any TLP. This is used during loopback mode to fill up the downstream queue.
28	**Address Translator Enable (ATE)** — R/W. This bit is used to enable address translation using the AT bits in this register during loopback mode. 0 = Disable 1 = Enable
27	Reserved
26	**Invalid Receive Bus Number Check Enable (IRBNCE)** — R/W. When set, the receive transaction layer will signal an error if the bus number of a Memory request does not fall within the range between SCBN and SBBN. If this check is enabled and the request is a memory write, it is treated as an Unsupported Request. If this check is enabled and the request is a non-posted memory read request, the request is considered a Malformed TLP and a fatal error. Messages, I/O, Config, and Completions are never checked for valid bus number.
25	**Invalid Receive Range Check Enable (IRRCE)** — R/W. When set, the receive transaction layer will treat the TLP as an Unsupported Request error if the address range of a Memory request does not outside the range between prefetchable and non-prefetchable base and limit. Messages, I/O, Configuration, and Completions are never checked for valid address ranges.



Bit	Description
24	**BME Receive Check Enable (BMERCE)** — R/W. When set, the receive transaction layer will treat the TLP as an Unsupported Request error if a memory read or write request is received and the Bus Master Enable bit is not set. Messages, I/O, Config, and Completions are never checked for BME.
23	Reserved
22	**Detect Override (FORCEDET)** — R/W. 0 = Normal operation. Detected output from AFE is sampled for presence detection. 1 = Override mode. Ignores AFE detect output and link training proceeds as if a device were detected.
21	**Flow Control During L1 Entry (FCDL1E)** — R/W. 0 = No flow control update DLLPs sent during L1 Ack transmission. 1 = Flow control update DLLPs sent during L1 Ack transmission as required to meet the 30 μs periodic flow control update.
20:18	**Unique Clock Exit Latency (UCEL)** — R/W. This value represents the L0s Exit Latency for unique-clock configurations (LCTL.CCC = 0) (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 50h:bit 6). It defaults to 512 ns to less than 1 μs, but may be overridden by BIOS.
17:15	**Common Clock Exit Latency (CCEL)** — R/W. This value represents the L0s Exit Latency for common-clock configurations (LCTL.CCC = 1) (D28:F0/F1/F2/F3/F4/F5/F6/F7:Offset 50h:bit 6). It defaults to 128 ns to less than 256 ns, but may be overridden by BIOS.
14	**PCIe Gen2 Speed Disable** — R/W. 0 = PCIe supported data rate is defined as set through Supported Link Speed and Target Link Speed settings. 1 = PCIe supported data rate is limited to 2.5 GT/s (Gen1). Supported Link Speed register bits will reflect "0001b" when this bit is set. When this bit is changed, link retrain needs to be performed for the change to be effective.
13:8	Reserved
7	**Port I/OxAPIC Enable (PAE)** — R/W. 0 = Hole is disabled. 1 = A range is opened through the bridge for the following memory addresses: **Port # — Address** 1 — FEC1_0000h – FEC1_7FFFh 2 — FEC1_8000h – FEC1_FFFFh 3 — FEC2_0000h – FEC2_7FFFh 4 — FEC2_8000h – FEC2_FFFFh 5 — FEC3_0000h – FEC3_7FFFh 6 — FEC3_8000h – FEC3_FFFFh 7 — FEC4_0000h – FEC4_7FFFh 8 — FEC4_8000h – FEC4_FFFFh
6:3	Reserved
2	**Bridge Type (BT)** — R/WO. This register can be used to modify the Base Class and Header Type fields from the default PCI-to-PCI bridge to a Host Bridge. Having the root port appear as a Host Bridge is useful in some server configurations. 0 = The root port bridge type is a PCI-to-PCI Bridge, Header Sub-Class = 04h, and Header Type = Type 1. 1 = The root port bridge type is a PCI-to-PCI Bridge, Header Sub-Class = 00h, and Header Type = Type 0.
1	**Hot-Plug SMI Enable (HPME)** — R/W. 0 = SMI generation based on a Hot-Plug event is disabled. 1 = Enables the root port to generate SMI whenever a Hot-Plug event is detected.
0	**Power Management SMI Enable (PMME)** — R/W. 0 = SMI generation based on a power management event is disabled. 1 = Enables the root port to generate SMI whenever a power management event is detected.

13.1.51 SMSCS—SMI/SCI Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: DCh–DFh
Attribute: R/WC
Default Value: 00000000h
Size: 32 bits

Bit	Description
31	**Power Management SCI Status (PMCS)** — R/WC. 1 = PME control logic needs to generate an interrupt, and this interrupt has been routed to generate an SCI.
30	**Hot-Plug SCI Status (HPCS)** — R/WC. 1 = Hot-Plug controller needs to generate an interrupt, and has this interrupt been routed to generate an SCI.
29:5	Reserved
4	**Hot-Plug Link Active State Changed SMI Status (HPLAS)** — R/WC. 1 = SLSTS.LASC (D28:F0/F1/F2/F3/F4/F5/F6/F7:5Ah, bit 8) transitioned from 0-to-1, and MPC.HPME (D28:F0/F1/F2/F3/F4/F5/F6/F7:D8h, bit 1) is set. When this bit is set, an SMI# will be generated.
3:2	Reserved
1	**Hot-Plug Presence Detect SMI Status (HPPDM)** — R/WC. 1 = SLSTS.PDC (D28:F0/F1/F2/F3/F4/F5/F6/F7:5Ah, bit 3) transitioned from 0-to-1, and MPC.HPME (D28:F0/F1/F2/F3/F4/F5/F6/F7:D8h, bit 1) is set. When this bit is set, an SMI# will be generated.
0	**Power Management SMI Status (PMMS)** — R/WC. 1 = RSTS.PS (D28:F0/F1/F2/F3/F4/F5/F6/F7:60h, bit 16) transitioned from 0-to-1, and MPC.PMME (D28:F0/F1/F2/F3/F4/F5/F6/F7:D8h, bit 1) is set.

13.1.52 RPDCGEN—Root Port Dynamic Clock Gating Enable Register (PCI Express—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: E1h
Attribute: R/W
Default Value: 00h
Size: 8-bits

Bits	Description
7:4	Reserved. RO
3	**Shared Resource Dynamic Link Clock Gating Enable (SRDLCGEN) —** R/W. 0 = Disables dynamic clock gating of the shared resource link clock domain. 1 = Enables dynamic clock gating on the root port shared resource link clock domain. Only the value from Port 1 is used for ports 1–4. Only the value from Port 5 is used for ports 5–8.
2	**Shared Resource Dynamic Backbone Clock Gate Enable (SRdBCGEN) —** R/W. 0 = Disables dynamic clock gating of the shared resource backbone clock domain. 1 = Enables dynamic clock gating on the root port shared resource backbone clock domain. Only the value from Port 1 is used for ports 1–4. Only the value from Port 5 is used for ports 5–8.
1	**Root Port Dynamic Link Clock Gate Enable (RPDLCGEN) —** R/W. 0 = Disables dynamic clock gating of the root port link clock domain. 1 = Enables dynamic clock gating on the root port link clock domain.
0	**Root Port Dynamic Backbone Clock Gate Enable (RPdBCGEN) —** R/W. 0 = Disables dynamic clock gating of the root port backbone clock domain. 1 = Enables dynamic clock gating on the root port backbone clock domain.

13.1.53 PECR3—PCI Express* Configuration Register 3 (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: ECh–EFh
Attribute: R/W
Default Value: 00000000h
Size: 32 bits

Bit	Description
31:2	Reserved
1	**Subtractive Decode Compatibility Device ID (SDCDID)** — R/W. 0 = This function reports the device Device ID value assigned to the PCI Express Root Ports. 1 = This function reports a Device ID of 244Eh. If subtractive decode (SDE) is enabled, having this bit as '0' allows the function to present a Device ID that is recognized by the operating system.
0	**Subtractive Decode Enable (SDE)** — R/W. 0 = Subtractive decode is disabled this function and will only claim transactions positively. 1 = This port will subtractively forward transactions across the PCIe link downstream memory and I/O transactions that are not positively claimed any internal device or bridge. Software must ensure that only one Intel® Xeon® Processor D-1500 Product Family device is enabled for Subtractive decode at a time.

13.1.54 UES—Uncorrectable Error Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 104h–107h
Attribute: R/WC, RO
Default Value: 00000000000x0xxx0x0x0000000x0000b
Size: 32 bits

This register maintains its state through a platform reset. It loses its state upon suspend.

Bit	Description
31:21	Reserved
20	**Unsupported Request Error Status (URE)** — R/WC. Indicates an unsupported request was received.
19	ECRC Error Status (EE) — RO. ECRC is not supported.
18	**Malformed TLP Status (MT)** — R/WC. Indicates a malformed TLP was received.
17	**Receiver Overflow Status (RO)** — R/WC. Indicates a receiver overflow occurred.
16	**Unexpected Completion Status (UC)** — R/WC. Indicates an unexpected completion was received.
15	**Completion Abort Status (CA)** — R/WC. Indicates a completer abort was received.
14	**Completion Timeout Status (CT)** — R/WC. Indicates a completion timed out. This bit is set if Completion Timeout is enabled and a completion is not returned within the time specified by the Completion TImeout Value
13	Flow Control Protocol Error Status (FCPE) — RO. Flow Control Protocol Errors not supported.
12	**Poisoned TLP Status (PT)** — R/WC. Indicates a poisoned TLP was received.
11:5	Reserved
4	**Data Link Protocol Error Status (DLPE)** — R/WC. Indicates a data link protocol error occurred.
3:1	Reserved
0	**Training Error Status (TE)** — RO. Training Errors not supported.

13.1.55 UEM—Uncorrectable Error Mask Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 108h–10Bh
Default Value: 00000000h
Attribute: R/WO, RO
Size: 32 bits

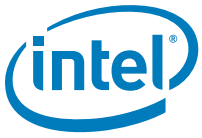
When set, the corresponding error in the UES register is masked, and the logged error will cause no action. When cleared, the corresponding error is enabled.

Bit	Description
31:21	Reserved
20	**Unsupported Request Error Mask (URE)** — R/WO. 0 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is enabled. 1 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is masked.
19	ECRC Error Mask (EE) — RO. ECRC is not supported.
18	**Malformed TLP Mask (MT)** — R/WO. 0 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is enabled. 1 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is masked.
17	**Receiver Overflow Mask (RO)** — R/WO. 0 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is enabled. 1 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is masked.
16	**Unexpected Completion Mask (UC)** — R/WO. 0 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is enabled. 1 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is masked.
15	**Completion Abort Mask (CA)** — R/WO. 0 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is enabled. 1 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is masked.
14	**Completion Timeout Mask (CT)** — R/WO. 0 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is enabled. 1 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is masked.
13	**Flow Control Protocol Error Mask (FCPE)** — RO. Flow Control Protocol Errors not supported.
12	**Poisoned TLP Mask (PT)** — R/WO. 0 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is enabled. 1 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is masked.
11:5	Reserved
4	**Data Link Protocol Error Mask (DLPE)** — R/WO. 0 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is enabled. 1 = The corresponding error in the UES register (D28:F0/F1/F2/F3/F4/F5/F6/F7:144) is masked.
3:1	Reserved
0	**Training Error Mask (TE)** — RO. Training Errors not supported

13.1.56 UEV—Uncorrectable Error Severity Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 10Ch–10Fh
Default Value: 00060011h
Attribute: RO, R/W
Size: 32 bits

Bit	Description
31:21	Reserved
20	**Unsupported Request Error Severity (URE)** — R/W. 0 = Error considered non-fatal. (Default) 1 = Error is fatal.
19	**ECRC Error Severity (EE)** — RO. ECRC is not supported.
18	**Malformed TLP Severity (MT)** — R/W. 0 = Error considered non-fatal. 1 = Error is fatal. (Default)



Bit	Description
17	**Receiver Overflow Severity (RO)** — R/W. 0 = Error considered non-fatal. 1 = Error is fatal. (Default)
16	Reserved
15	**Completion Abort Severity (CA)** — R/W. 0 = Error considered non-fatal. (Default) 1 = Error is fatal.
14	Reserved
13	**Flow Control Protocol Error Severity (FCPE)** — RO. Flow Control Protocol Errors not supported.
12	**Poisoned TLP Severity (PT)** — R/W. 0 = Error considered non-fatal. (Default) 1 = Error is fatal.
11:5	Reserved
4	**Data Link Protocol Error Severity (DLPE)** — R/W. 0 = Error considered non-fatal. 1 = Error is fatal. (Default)
3:1	Reserved
0	Training Error Severity (TE) — R/W. TE is not supported.

13.1.57 CES—Correctable Error Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 110h–113h
Attribute: R/WC
Default Value: 00000000h
Size: 32 bits

Bit	Description
31:14	Reserved
13	**Advisory Non-Fatal Error Status (ANFES)** — R/WC. 0 = Advisory Non-Fatal Error did not occur. 1 = Advisory Non-Fatal Error did occur.
12	**Replay Timer Timeout Status (RTT)** — R/WC. Indicates the replay timer timed out.
11:9	Reserved
8	**Replay Number Rollover Status (RNR)** — R/WC. Indicates the replay number rolled over.
7	**Bad DLLP Status (BD)** — R/WC. Indicates a bad DLLP was received.
6	**Bad TLP Status (BT)** — R/WC. Indicates a bad TLP was received.
5:1	Reserved
0	**Receiver Error Status (RE)** — R/WC. Indicates a receiver error occurred.

13.1.58 CEM—Correctable Error Mask Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 114h–117h
Default Value: 00002000h
Attribute: R/WO
Size: 32 bits

When set, the corresponding error in the CES register is masked, and the logged error will cause no action. When cleared, the corresponding error is enabled.

Bit	Description
31:14	Reserved
13	**Advisory Non-Fatal Error Mask (ANFEM)** — R/WO. 0 = Does not mask Advisory Non-Fatal errors. 1 = Masks Advisory Non-Fatal errors from (a) signaling ERR_COR to the device control register and (b) updating the Uncorrectable Error Status register. This register is set by default to enable compatibility with software that does not comprehend Role-Based Error Reporting. ***Note:*** The correctable error detected bit in device status register is set whenever the Advisory Non-Fatal error is detected, independent of this mask bit.
12	**Replay Timer Timeout Mask (RTT)** — R/WO. Mask for replay timer timeout.
11:9	Reserved
8	**Replay Number Rollover Mask (RNR)** — R/WO. Mask for replay number rollover.
7	**Bad DLLP Mask (BD)** — R/WO. Mask for bad DLLP reception.
6	**Bad TLP Mask (BT)** — R/WO. Mask for bad TLP reception.
5:1	Reserved
0	**Receiver Error Mask (RE)** — R/WO. Mask for receiver errors.

13.1.59 AECC—Advanced Error Capabilities and Control Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

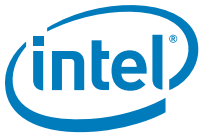
Address Offset: 118h–11Bh
Default Value: 00000000h
Attribute: RO
Size: 32 bits

Bit	Description
31:9	Reserved
8	ECRC Check Enable (ECE) — RO. ECRC is not supported.
7	ECRC Check Capable (ECC) — RO. ECRC is not supported.
6	ECRC Generation Enable (EGE) — RO. ECRC is not supported.
5	ECRC Generation Capable (EGC) — RO. ECRC is not supported.
4:0	First Error Pointer (FEP) — RO. Identifies the bit position of the last error reported in the Uncorrectable Error Status Register.

13.1.60 RES—Root Error Status Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 130h–133h
Default Value: 00000000h
Attribute: R/WC, RO
Size: 32 bits

Bit	Description
31:27	**Advanced Error Interrupt Message Number (AEMN)** — RO. There is only one error interrupt allocated.
26:7	Reserved
6	**Fatal Error Messages Received (FEMR)** — RO. Set when one or more Fatal Uncorrectable Error Messages have been received.
5	**Non-Fatal Error Messages Received (NFEMR)—** RO. Set when one or more Non-Fatal Uncorrectable error messages have been received



Bit	Description
4	**First Uncorrectable Fatal (FUF)—** RO. Set when the first Uncorrectable Error message received is for a fatal error.
3	**Multiple ERR_FATAL/NONFATAL Received (MENR)** — RO. For Intel® Xeon® Processor D-1500 Product Family, only one error will be captured.
2	**ERR_FATAL/NONFATAL Received (ENR)** — R/WC. 0 = No error message received. 1 = Either a fatal or a non-fatal error message is received.
1	**Multiple ERR_COR Received (MCR)** — RO. For Intel® Xeon® Processor D-1500 Product Family, only one error will be captured.
0	**ERR_COR Received (CR)** — R/WC. 0 = No error message received. 1 = A correctable error message is received.

13.1.61 PECR2—PCI Express* Configuration Register 2 (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 320–323h Attribute: R/W
Default Value: 0004B05Bh Size: 32 bits

Bit	Description
31:20	Reserved
21	**PECR2 Field 1** — R/W. BIOS must set this bit to 1b.
20:0	Reserved

13.1.62 PEETM—PCI Express* Extended Test Mode Register (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 324h–327h Attribute: RO
Default Value: See Description Size: 32 bits

Bit	Description
31:5	Reserved
4	**Lane Reversal (LR)** — RO. This register reads the setting of the PCIELR1 soft strap for port 1 and the PCIELR2 soft strap for port 5. 0 = No Lane reversal (default). 1 = PCI Express lanes 0-3 (register in port 1) or lanes 4-7 (register in port 5) are reversed. ***Notes:*** 1. The port configuration straps must be set such that Port 1 or Port 5 is configured as a x4 port using lanes 0–3, or 4–7 when Lane Reversal is enabled. x2 lane reversal is not supported. 2. This register is only valid on port 1 (for ports 1–4) or port 5 (for ports 5–8).
3	Reserved
2	**Scrambler Bypass Mode (BAU)** — R/W. 0 = Normal operation. Scrambler and descrambler are used. 1 = Bypasses the data scrambler in the transmit direction and the data de-scrambler in the receive direction. ***Note:*** This functionality intended for debug/testing only. ***Note:*** If bypassing scrambler with Intel® Xeon® Processor D-1500 Product Family root port 1 in x4 configuration, each Intel® Xeon® Processor D-1500 Product Family root port must have this bit set.
1:0	Reserved

13.1.63 PEC1—PCI Express* Configuration Register 1 (PCI Express*—D28:F0/F1/F2/F3/F4/F5/F6/F7)

Address Offset: 330h–333h
Attribute: RO, R/W
Default Value: 28000016h
Size: 32 bits

Bit	Description
31:8	Reserved
7:0	**PEC1 Field 1** — R/W. BIOS must program this field to 40h.

§

14 High Precision Event Timer Registers

The timer registers are memory-mapped in a non-indexed scheme. This allows the processor to directly access each register without having to use an index register. The timer register space is 1024 bytes. The registers are generally aligned on 64-bit boundaries to simplify implementation with IA64 processors. There are four possible memory address ranges beginning at 1) FED0_0000h, 2) FED0_1000h, 3) FED0_2000h, 4) FED0_3000h. The choice of address range will be selected by configuration bits in the High Precision Timer Configuration Register (Chipset Config Registers:Offset 3404h).

Behavioral Rules:

1. Software must not attempt to read or write across register boundaries. For example, a 32-bit access should be to offset x0h, x4h, x8h, or xCh. 32-bit accesses should not be to 01h, 02h, 03h, 05h, 06h, 07h, 09h, 0Ah, 0Bh, 0Dh, 0Eh, or 0Fh. Any accesses to these offsets will result in an unexpected behavior, and may result in a master abort. However, these accesses should not result in system hangs. 64-bit accesses can only be to x0h and must not cross 64-bit boundaries.
2. Software should not write to Read Only registers.
3. Software should not expect any particular or consistent value when reading reserved registers or bits.

14.1 Memory Mapped Registers

Table 14-1. Memory-Mapped Register Address Map (Sheet 1 of 2)

Offset	Mnemonic	Register	Default	Attribute
000h–007h	GCAP_ID	General Capabilities and Identification	0429B17F8086 A201h	RO
008h–00Fh	—	Reserved	—	—
010h–017h	GEN_CONF	General Configuration	0000000000000000h	R/W
018h–01Fh	—	Reserved	—	—
020h–027h	GINTR_STA	General Interrupt Status	0000000000000000h	R/WC
028h–0EFh	—	Reserved	—	—
0F0h–0F7h	MAIN_CNT	Main Counter Value	N/A	R/W
0F8h–0FFh	—	Reserved	—	—
100h–107h	TIM0_CONF	Timer 0 Configuration and Capabilities	N/A	R/W, RO
108h–10Fh	TIM0_COMP	Timer 0 Comparator Value	N/A	R/W
110h–11Fh	—	Reserved	—	—
120h–127h	TIM1_CONF	Timer 1 Configuration and Capabilities	N/A	R/W, RO
128h–12Fh	TIM1_COMP	Timer 1 Comparator Value	N/A	R/W
130h–13Fh	—	Reserved	—	—
140h–147h	TIM2_CONF	Timer 2 Configuration and Capabilities	N/A	R/W, RO
148h–14Fh	TIM2_COMP	Timer 2 Comparator Value	N/A	R/W
150h–15Fh	—	Reserved	—	—

Table 14-1. Memory-Mapped Register Address Map (Sheet 2 of 2)

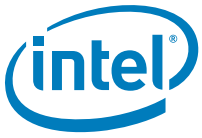
Offset	Mnemonic	Register	Default	Attribute
160h–167h	TIM3_CONG	Timer 3 Configuration and Capabilities	N/A	R/W, RO
168h–16Fh	TIM3_COMP	Timer 3 Comparator Value	N/A	R/W
180h–187h	TIM4_CONG	Timer 4 Configuration and Capabilities	N/A	R/W, RO
188h–18Fh	TIM4_COMP	Timer 4 Comparator Value	N/A	R/W
190h–19Fh	—	Reserved	—	—
1A0h–1A7h	TIM5_CONG	Timer 5 Configuration and Capabilities	N/A	R/W, RO
1A8h–1AFh	TIM5_COMP	Timer 5 Comparator Value	N/A	R/W
1B0h–1BFh	—	Reserved	—	—
1C0h–1C7h	TIM6_CONG	Timer 6 Configuration and Capabilities	N/A	R/W, RO
1C8h–1CFh	TIM6_COMP	Timer 6 Comparator Value	N/A	R/W
1D0h–1DFh	—	Reserved	—	—
1E0h–1E7h	TIM7_CONG	Timer 7 Configuration and Capabilities	N/A	R/W, RO
1E8h–1EFh	TIM7_COMP	Timer 7 Comparator Value	N/A	R/W
1F0h–19Fh	—	Reserved	—	—
200h–3FFh	—	Reserved	—	—

Notes:
1. Reads to reserved registers or bits will return a value of 0.
2. Software must not attempt locks to the memory-mapped I/O ranges for High Precision Event Timers. If attempted, the lock is not honored, which means potential deadlock conditions may occur.

14.1.1 GCAP_ID—General Capabilities and Identification Register

Address Offset: 00h Attribute: RO
Default Value: 0429B17F8086A201h Size: 64 bits

Bit	Description
63:32	Main Counter Tick Period (COUNTER_CLK_PER_CAP) — RO. This field indicates the period at which the counter increments in femptoseconds (10^-15 seconds). This will return 0429B17Fh when read. This indicates a period of 69841279 fs (69.841279 ns).
31:16	Vendor ID Capability (VENDOR_ID_CAP) — RO. This is a 16-bit value assigned to Intel.
15	Legacy Replacement Rout Capable (LEG_RT_CAP) — RO. Hardwired to 1. Legacy Replacement Interrupt Rout option is supported.
14	Reserved. This bit returns 0 when read.
13	Counter Size Capability (COUNT_SIZE_CAP) — RO. Hardwired to 1. Counter is 64-bit wide.
12:8	Number of Timer Capability (NUM_TIM_CAP) — RO. This field indicates the number of timers in this block. 07h = Eight timers.
7:0	Revision Identification (REV_ID) — RO. This indicates which revision of the function is implemented. Default value will be 01h.



14.1.2 GEN_CONF—General Configuration Register

Address Offset: 010h Attribute: R/W
Default Value: 00000000 00000000h Size: 64 bits

Bit	Description
63:2	Reserved. These bits return 0 when read.
1	**Legacy Replacement Rout (LEG_RT_CNF)** — R/W. If the ENABLE_CNF bit and the LEG_RT_CNF bit are both set, then the interrupts will be routed as follows: • Timer 0 is routed to IRQ0 in 8259 or IRQ2 in the I/O APIC • Timer 1 is routed to IRQ8 in 8259 or IRQ8 in the I/O APIC • Timer 2-n is routed as per the routing in the timer n config registers. • If the Legacy Replacement Rout bit is set, the individual routing bits for Timers 0 and 1 (APIC) will have no impact. • If the Legacy Replacement Rout bit is not set, the individual routing bits for each of the timers are used. • This bit will default to 0. BIOS can set it to 1 to enable the legacy replacement routing, or 0 to disable the legacy replacement routing.
0	**Overall Enable (ENABLE_CNF)** — R/W. This bit must be set to enable any of the timers to generate interrupts. If this bit is 0, then the main counter will halt (will not increment) and no interrupts will be caused by any of these timers. For level-triggered interrupts, if an interrupt is pending when the ENABLE_CNF bit is changed from 1 to 0, the interrupt status indications (in the various Txx_INT_STS bits) will not be cleared. Software must write to the Txx_INT_STS bits to clear the interrupts. ***Note:*** This bit will default to 0. BIOS can set it to 1 or 0.

14.1.3 GINTR_STA—General Interrupt Status Register

Address Offset: 020h Attribute: R/WC
Default Value: 00000000 00000000h Size: 64 bits

Bit	Description
63:8	Reserved. These bits will return 0 when read.
7	**Timer 7 Interrupt Active (T07_INT_STS)** — R/WC. Same functionality as Timer 0.
6	**Timer 6 Interrupt Active (T06_INT_STS)** — R/WC. Same functionality as Timer 0.
5	**Timer 5 Interrupt Active (T05_INT_STS)** — R/WC. Same functionality as Timer 0.
4	**Timer 4 Interrupt Active (T04_INT_STS)** — R/WC. Same functionality as Timer 0.
3	**Timer 3 Interrupt Active (T03_INT_STS)** — R/WC. Same functionality as Timer 0.
2	**Timer 2 Interrupt Active (T02_INT_STS)** — R/WC. Same functionality as Timer 0.
1	**Timer 1 Interrupt Active (T01_INT_STS)** — R/WC. Same functionality as Timer 0.
0	**Timer 0 Interrupt Active (T00_INT_STS)** — R/WC. The functionality of this bit depends on whether the edge or level-triggered mode is used for this timer. (default = 0) If set to level-triggered mode: This bit will be set by hardware if the corresponding timer interrupt is active. Once the bit is set, it can be cleared by software writing a 1 to the same bit position. Writes of 0 to this bit will have no effect. If set to edge-triggered mode: This bit should be ignored by software. Software should always write 0 to this bit. ***Note:*** Defaults to 0. In edge triggered mode, this bit will always read as 0 and writes will have no effect.

14.1.4 MAIN_CNT—Main Counter Value Register

Address Offset: 0F0h Attribute: R/W
Default Value: N/A Size: 64 bits

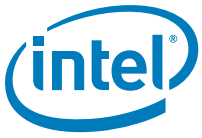
Bit	Description
63:0	**Counter Value (COUNTER_VAL[63:0])** — R/W. Reads return the current value of the counter. Writes load the new value to the counter. ***Notes:*** 1. Writes to this register should only be done while the counter is halted. 2. Reads to this register return the current value of the main counter. 3. 32-bit counters will always return 0 for the upper 32-bits of this register. 4. If 32-bit software attempts to read a 64-bit counter, it should first halt the counter. Since this delays the interrupts for all of the timers, this should be done only if the consequences are understood. It is strongly recommended that 32-bit software only operate the timer in 32-bit mode. 5. Reads to this register are monotonic. No two consecutive reads return the same value. The second of two reads always returns a larger value (unless the timer has rolled over to 0).

14.1.5 TIMn_CONF—Timer n Configuration and Capabilities Register

Address Offset: Timer 0: 100–107h, Attribute: RO, R/W
Timer 1: 120–127h,
Timer 2: 140–147h,
Timer 3: 160–167h,
Timer 4: 180–187h,
Timer 5: 1A0–1A7h,
Timer 6: 1C0–1C7h,
Timer 7: 1E0–1E7h,
Default Value: N/A Size: 64 bit

Note: The letter n can be 0, 1, 2, 3, 4, 5, 6, or 7 referring to Timer 0, 1, 2, 3, 4, 5, 6, or 7.

Bit	Description
63:56	Reserved. These bits will return 0 when read.
55:52, 44,43	**Timer Interrupt Rout Capability (TIMERn_INT_ROUT_CAP)** — RO. Timer 0, 1:Bits 52, 53, 54, and 55 in this field (corresponding to IRQ 20, 21, 22, and 23) have a value of 1. Writes will have no effect. Timer 2:Bits 43, 52, 53, 54, and 55 in this field (corresponding to IRQ 11, 20, 21, 22, and 23) have a value of 1. Writes will have no effect. Timer 3:Bits 44, 52, 53, 54, and 55 in this field (corresponding to IRQ 11, 20, 21, 22, and 23) have a value of 1. Writes will have no effect. Timer 4, 5, 6, 7:This field is always 0 as interrupts from these timers can only be delivered using direct processor interrupt messages. ***Note:*** If IRQ 11 is used for HPET #2, software should ensure IRQ 11 is not shared with any other devices to ensure the proper operation of HPET #2. ***Note:*** If IRQ 12 is used for HPET #3, software should ensure IRQ 12 is not shared with any other devices to ensure the proper operation of HPET #3.
51:45, 42:16	Reserved**.** These bits return 0 when read.
15	**Timer n Processor Message Interrupt Delivery (Tn_PROCMSG_INT_DEL_CAP)** — RO. This bit is always read as '1', since Intel® Xeon® Processor D-1500 Product Family HPET implementation supports the direct processor interrupt delivery.
14	**Timer n Processor Message Interrupt Enable (Tn_PROCMSG_EN_CNF)** — R/W / RO. If the Tn_PROCMSG_INT_DEL_CAP bit is set for this timer, then the software can set the Tn_PROCMSG_EN_CNF bit to force the interrupts to be delivered directly as processor messages, rather than using the 8259 or I/O (x) APIC. In this case, the Tn_INT_ROUT_CNF field in this register will be ignored. The Tn_PROCMSG_ROUT register will be used instead. Timer 0, 1, 2, 3 Specific: This bit is a read/write bit. Timer 4, 5, 6, 7 Specific: This bit is always Read Only '1' as interrupt from these timers can only be delivered using direct processor interrupt messages.



Bit	Description
13:9	**Timer n Interrupt Rout (Tn_INT_ROUT_CNF)** — R/W / RO. This 5-bit field indicates the routing for the interrupt to the 8259 or I/O (x) APIC. Software writes to this field to select which interrupt in the 8259 or I/O (x) will be used for this timer's interrupt. If the value is not supported by this particular timer, then the value read back will not match what is written. The software must only write valid values. Timer 4, 5, 6, 7: This field is Read Only and reads will return 0. ***Notes:*** 1. If the interrupt is handled using the 8259, only interrupts 0–15 are applicable and valid. Software must not program any value other than 0–15 in this field. 2. If the Legacy Replacement Rout bit is set, then Timers 0 and 1 will have a different routing, and this bit field has no effect for those two timers. 3. Timer 0,1: Software is responsible to make sure it programs a valid value (20, 21, 22, or 23) for this field. Intel® Xeon® Processor D-1500 Product Family logic does not check the validity of the value written. 4. Timer 2: Software is responsible to make sure it programs a valid value (11, 20, 21, 22, or 23) for this field. Intel® Xeon® Processor D-1500 Product Family logic does not check the validity of the value written. 5. Timer 3: Software is responsible to make sure it programs a valid value (12, 20, 21, 22, or 23) for this field. Intel® Xeon® Processor D-1500 Product Family logic does not check the validity of the value written. 6. Timers 4, 5, 6, 7: This field is always Read Only 0 as interrupts from these timers can only be delivered using direct processor interrupt messages.
8	**Timer n 32-bit Mode (TIMERn_32MODE_CNF)** — R/W or RO. Software can set this bit to force a 64-bit timer to behave as a 32-bit timer. Timer 0:Bit is read/write (default to 0). 0 = 64 bit; 1 = 32 bit Timers 1, 2, 3, 4, 5, 6, 7:Hardwired to 0. Writes have no effect (since these seven timers are 32-bits). ***Note:*** When this bit is set to 1, the hardware counter will do a 32-bit operation on comparator match and rollovers; thus, the upper 32-bit of the Timer 0 Comparator Value register is ignored. The upper 32-bit of the main counter is not involved in any rollover from lower 32-bit of the main counter and becomes all zeros.
7	Reserved**.** This bit returns 0 when read.
6	**Timer n Value Set (TIMERn_VAL_SET_CNF)** — R/W. Software uses this bit only for Timer 0 if it has been set to periodic mode. By writing this bit to a 1, the software is then allowed to directly set the timer's accumulator. Software does **not** have to write this bit back to 1 (it automatically clears). Software should not write a 1 to this bit position if the timer is set to non-periodic mode. ***Note:*** This bit will return 0 when read. Writes will only have an effect for Timer 0 if it is set to periodic mode. Writes will have no effect for Timers 1, 2, 3, 4, 5, 6, 7.
5	**Timer n Size (TIMERn_SIZE_CAP)** — RO. This read only field indicates the size of the timer. Timer 0:Value is 1 (64-bits). Timers 1, 2, 3, 4, 5, 6, 7: Value is 0 (32-bits).
4	**Periodic Interrupt Capable (TIMERn_PER_INT_CAP)** — RO. If this bit is 1, the hardware supports a periodic mode for this timer's interrupt. Timer 0: Hardwired to 1 (supports the periodic interrupt). Timers 1, 2, 3, 4, 5, 6, 7: Hardwired to 0 (does not support periodic interrupt).
3	**Timer n Type (TIMERn_TYPE_CNF)** — R/W or RO. Timer 0:Bit is read/write. 0 = Disable timer to generate periodic interrupt; 1 = Enable timer to generate a periodic interrupt. Timers 1, 2, 3, 4, 5, 6, 7: Hardwired to 0. Writes have no affect.
2	**Timer n Interrupt Enable (TIMERn_INT_ENB_CNF)** — R/W. This bit must be set to enable timer n to cause an interrupt when it times out. 0 = Disable (Default). The timer can still count and generate appropriate status bits, but will not cause an interrupt. 1 = Enable.

Bit	Description
1	**Timer Interrupt Type (TIMERn_INT_TYPE_CNF)** — R/W. 0 = The timer interrupt is edge triggered. This means that an edge-type interrupt is generated. If another interrupt occurs, another edge will be generated. 1 = The timer interrupt is level triggered. This means that a level-triggered interrupt is generated. The interrupt will be held active until it is cleared by writing to the bit in the General Interrupt Status Register. If another interrupt occurs before the interrupt is cleared, the interrupt will remain active. Timer 4, 5, 6, 7: This bit is Read Only, and will return 0 when read
0	Reserved**.** These bits will return 0 when read.

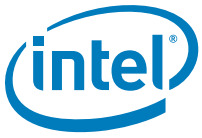
Note: Reads or writes to unimplemented timers should not be attempted. Read from any unimplemented registers will return an undetermined value.

14.1.6 TIMn_COMP—Timer n Comparator Value Register

Address Offset: Timer 0: 108h–10Fh,
Timer 1: 128h–12Fh,
Timer 2: 148h–14Fh,
Timer 3: 168h–16Fh,
Timer 4: 188h–18Fh,
Timer 5: 1A8h–1AFh,
Timer 6: 1C8h–1CFh,
Timer 7: 1E8h–1EFh

Attribute: R/W
Default Value: N/A Size: 64 bit

Bit	Description
63:0	**Timer Compare Value** — R/W. Reads to this register return the current value of the comparator If Timer n is configured to non-periodic mode: Writes to this register load the value against which the main counter should be compared for this timer. • When the main counter equals the value last written to this register, the corresponding interrupt can be generated (if so enabled). • The value in this register does not change based on the interrupt being generated. If Timer 0 is configured to periodic mode: • When the main counter equals the value last written to this register, the corresponding interrupt can be generated (if so enabled). • After the main counter equals the value in this register, the value in this register is increased by the value last written to the register. For example, if the value written to the register is 00000123h, then 1. An interrupt will be generated when the main counter reaches 00000123h. 2. The value in this register will then be adjusted by the hardware to 00000246h. 3. Another interrupt will be generated when the main counter reaches 00000246h 4. The value in this register will then be adjusted by the hardware to 00000369h • As each periodic interrupt occurs, the value in this register will increment. When the incremented value is greater than the maximum value possible for this register (FFFFFFFFh for a 32-bit timer or FFFFFFFFFFFFFFFFh for a 64-bit timer), the value will wrap around through 0. For example, if the current value in a 32-bit timer is FFFF0000h and the last value written to this register is 20000h, then after the next interrupt the value will change to 00010000h Default value for each timer is all 1s for the bits that are implemented. For example, a 32-bit timer has a default value of 00000000FFFFFFFFh. A 64-bit timer has a default value of FFFFFFFFFFFFFFFFh.



14.1.7 TIMERn_PROCMSG_ROUT—Timer n Processor Message Interrupt Rout Register

Address Offset:	Timer 0: 110–117h, Timer 1: 130–137h, Timer 2: 150–157h, Timer 3: 170–177h, Timer 4: 190–197h, Timer 5: 1B0–1B7h, Timer 6: 1D0–1D7h, Timer 7: 1F0–1F7h,	Attribute:	R/W
Default Value:	N/A	Size:	64 bit

Note: The letter n can be 0, 1, 2, 3, 4, 5, 6, or 7 referring to Timer 0, 1, 2, 3, 4, 5, 6, or 7.

Software can access the various bytes in this register using 32-bit or 64-bit accesses. 32-bit accesses can be done to offset 1x0h or 1x4h. 64-bit accesses can be done to 1x0h. 32-bit accesses must not be done to offsets 1x1h, 1x2h, 1x3h, 1x5h, 1x6h, or 1x7h.

Bit	Description
63:32	**Tn_PROCMSG_INT_ADDR** — R/W. Software sets this 32-bit field to indicate the location that the direct processor interrupt message should be written.
31:0	**Tn_PROCMSG_INT_VAL** — R/W. Software sets this 32-bit field to indicate that value that is written during the direct processor interrupt message.

§

15 Serial Peripheral Interface (SPI)

The Serial Peripheral Interface resides in memory mapped space. This function contains registers that allow for the setup and programming of devices that reside on the SPI interface.

Note: All registers in this function (including memory-mapped registers) must be addressable in byte, word, and DWord quantities. The software must always make register accesses on natural boundaries (that is, DWord accesses must be on DWord boundaries; word accesses on word boundaries, and so on) In addition, the memory-mapped register space must not be accessed with the LOCK semantic exclusive-access mechanism. If software attempts exclusive-access mechanisms to the SPI memory-mapped space, the results are undefined.

15.1 Serial Peripheral Interface Memory Mapped Configuration Registers

The SPI Host Interface registers are memory-mapped in the RCRB (Root Complex Register Block) Chipset Register Space with a base address (SPIBAR) of 3800h and are located within the range of 3800h to 39FFh. The address for RCRB are in the RCBA Register (see Section 7.1.40). The individual registers are then accessible at SPIBAR + Offset as indicated in the following table.

These memory mapped registers must be accessed in byte, word, or DWord quantities.

Table 15-1. Serial Peripheral Interface (SPI) Register Address Map (SPI Memory Mapped Configuration Registers) (Sheet 1 of 2)

SPIBAR + Offset	Mnemonic	Register Name	Default
00h–03h	BFPR	BIOS Flash Primary Region	00000000h
04h–05h	HSFS	Hardware Sequencing Flash Status	0000h
06h–07h	HSFC	Hardware Sequencing Flash Control	0000h
08h–0Bh	FADDR	Flash Address	00000000h
0Ch–0Fh	—	Reserved	00000000h
10h–13h	FDATA0	Flash Data 0	00000000h
14h–4Fh	FDATAN	Flash Data N	00000000h
50h–53h	FRAP	Flash Region Access Permissions	00000202h
54h–57h	FREG0	Flash Region 0	00000000h
58h–5Bh	FREG1	Flash Region 1	00000000h
5Ch–5Fh	FREG2	Flash Region 2	00000000h
60h–63h	FREG3	Flash Region 3	00000000h
64h–67h	FREG4	Flash Region 4	00000000h
67h–73h	—	Reserved for Future Flash Regions	
74h–77h	PR0	Flash Protected Range 0	00000000h
78h–7Bh	PR1	Flash Protected Range 1	00000000h
7Ch–7Fh	PR2	Flash Protected Range 2	00000000h

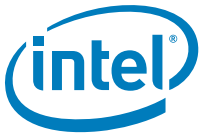


Table 15-1. Serial Peripheral Interface (SPI) Register Address Map (SPI Memory Mapped Configuration Registers) (Sheet 2 of 2)

SPIBAR + Offset	Mnemonic	Register Name	Default
80h–83h	PR3	Flash Protected Range 3	00000000h
84h–87h	PR4	Flash Protected Range 4	00000000h
88h–8Fh	—	Reserved	—
90h	SSFS	Software Sequencing Flash Status	00h
91h–93h	SSFC	Software Sequencing Flash Control	0000h
94h–95h	PREOP	Prefix Opcode Configuration	0000h
96h–97h	OPTYPE	Opcode Type Configuration	0000h
98h–9Fh	OPMENU	Opcode Menu Configuration	0000000000000000h
A0h	BBAR	BIOS Base Address Configuration	00000000h
B0h–B3h	FDOC	Flash Descriptor Observability Control	00000000h
B4h–B7h	FDOD	Flash Descriptor Observability Data	00000000h
B8h–C3h	—	Reserved	—
C0h–C3h	AFC	Additional Flash Control	00000000h
C4h–C7h	LVSCC	Host Lower Vendor Specific Component Capabilities	00000000h
C8h–C11h	UVSCC	Host Upper Vendor Specific Component Capabilities	00000000h
D0h–D3h	FPB	Flash Partition Boundary	00000000h
F0h–F3h	SRDL	Soft Reset Data Lock	00000000h
F4h–F7h	SRDC	Soft Reset Data Control	00000000h
F8h–FBh	SRD	Soft Reset Data	00000000h

15.1.1 BFPR –BIOS Flash Primary Region Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 00h Attribute: RO
Default Value: 00000000h Size: 32 bits

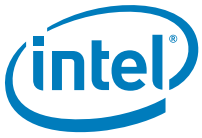
Note: This register is only applicable when SPI device is in descriptor mode.

Bit	Description
31:29	Reserved
28:16	**BIOS Flash Primary Region Limit (PRL) —** RO. This specifies address bits 24:12 for the Primary Region Limit. The value in this register loaded from the contents in the Flash Descriptor.FLREG1.Region Limit
15:13	Reserved
12:0	**BIOS Flash Primary Region Base (PRB)** — RO. This specifies address bits 24:12 for the Primary Region Base The value in this register is loaded from the contents in the Flash Descriptor.FLREG1.Region Base

15.1.2 HSFS—Hardware Sequencing Flash Status Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 04h
Default Value: 0000h
Attribute: RO, R/WC, R/W
Size: 16 bits

Bit	Description
15	**Flash Configuration Lock-Down (FLOCKDN)** — R/W/L. When set to 1, those Flash Program Registers that are locked down by this FLOCKDN bit cannot be written. Once set to 1, this bit can only be cleared by a hardware reset due to a global reset or host partition reset in an Intel ME enabled system.
14	**Flash Descriptor Valid (FDV) —** RO. This bit is set to a 1 if the Flash Controller read the correct Flash Descriptor Signature. If the Flash Descriptor Valid bit is not 1, software cannot use the Hardware Sequencing registers, but must use the software sequencing registers. Any attempt to use the Hardware Sequencing registers will result in the FCERR bit being set.
13	**Flash Descriptor Override Pin Strap Status (FDOPSS)** — RO. This bit indicates the condition of the Flash Descriptor Security Override / Intel ME Debug Mode pin strap. 0 = The Flash Descriptor Security Override / Intel ME Debug Mode strap is set using external pull-up on MFG_MODE_STRAP 1 = No override
12:6	Reserved
5	**SPI Cycle In Progress (SCIP)—** RO. Hardware sets this bit when software sets the Flash Cycle Go (FGO) bit in the Hardware Sequencing Flash Control register. This bit remains set until the cycle completes on the SPI interface. Hardware automatically sets and clears this bit so that software can determine when read data is valid and/or when it is safe to begin programming the next command. Software must only program the next command when this bit is 0. ***Note:*** This field is only applicable when in Descriptor mode and Hardware sequencing is being used.
4:3	**Block/Sector Erase Size (BERASE)** — RO. This field identifies the erasable sector size for all Flash components. Valid Bit Settings: 00 = 256 Byte 01 = 4 K Byte 10 = 8 K Byte 11 = 64 K Byte If the FLA is less than FPBA, then this field reflects the value in the LVSCC.LBES register. If the FLA is greater or equal to FPBA, then this field reflects the value in the UVSCC.UBES register. ***Note:*** This field is only applicable when in Descriptor mode and Hardware sequencing is being used.
2	**Access Error Log (AEL)** — R/W/C. Hardware sets this bit to a 1 when an attempt was made to access the BIOS region using the direct access method or an access to the BIOS Program Registers that violated the security restrictions. This bit is simply a log of an access security violation. This bit is cleared by software writing a 1. ***Note:*** This field is only applicable when in Descriptor mode and Hardware sequencing is being used.
1	**Flash Cycle Error (FCERR)** — R/W/C. Hardware sets this bit to 1 when an program register access is blocked to the FLASH due to one of the protection policies or when any of the programmed cycle registers is written while a programmed access is already in progress. This bit remains asserted until cleared by software writing a 1 or until hardware reset occurs due to a global reset or host partition reset in an Intel® ME enabled system. Software must clear this bit before setting the FLASH Cycle GO bit in this register. ***Note:*** This field is only applicable when in Descriptor mode and Hardware sequencing is being used.
0	**Flash Cycle Done (FDONE)** — R/W/C. Intel® Xeon® Processor D-1500 Product Family sets this bit to 1 when the SPI Cycle completes after software previously set the FGO bit. This bit remains asserted until cleared by software writing a 1 or hardware reset due to a global reset or host partition reset in an Intel ME enabled system. When this bit is set and the SPI SMI# Enable bit is set, an internal signal is asserted to the SMI# generation block. Software must make sure this bit is cleared prior to enabling the SPI SMI# assertion for a new programmed access. ***Note:*** This field is only applicable when in Descriptor mode and Hardware sequencing is being used.



15.1.3 HSFC—Hardware Sequencing Flash Control Register (SPI Memory Mapped Configuration Registers)

Memory Address:	SPIBAR + 06h	Attribute:	R/W, R/WS
Default Value:	0000h	Size:	16 bits

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

Bit	Description
15	**Flash SPI SMI# Enable (FSMIE)** — R/W. When set to 1, the SPI asserts an SMI# request whenever the Flash Cycle Done bit is 1.
14	Reserved
13:8	**Flash Data Byte Count (FdBC) —** R/W. This field specifies the number of bytes to shift in or out during the data portion of the SPI cycle. The contents of this register are 0s based with 0b representing 1 byte and 111111b representing 64 bytes. The number of bytes transferred is the value of this field plus 1. This field is ignored for the Block Erase command.
7:3	Reserved
2:1	**FLASH Cycle (FCYCLE)** — R/W. This field defines the Flash SPI cycle type generated to the FLASH when the FGO bit is set as defined below: 00 = Read (1 up to 64 bytes by setting FdBC) 01 = Reserved 10 = Write (1 up to 64 bytes by setting FdBC) 11 = Block Erase
0	**Flash Cycle Go (FGO)** — R/W/S. A write to this register with a 1 in this bit initiates a request to the Flash SPI Arbiter to start a cycle. This register is cleared by hardware when the cycle is granted by the SPI arbiter to run the cycle on the SPI bus. When the cycle is complete, the FDONE bit is set. Software is forbidden to write to any register in the HSFLCTL register between the FGO bit getting set and the FDONE bit being cleared. Any attempt to violate this rule will be ignored by hardware. Hardware allows other bits in this register to be programmed for the same transaction when writing this bit to 1. This saves an additional memory write. This bit always returns 0 on reads.

15.1.4 FADDR—Flash Address Register (SPI Memory Mapped Configuration Registers)

Memory Address:	SPIBAR + 08h	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits

Bit	Description
31:25	Reserved
24:0	**Flash Linear Address (FLA) —** R/W. The FLA is the starting byte linear address of a SPI Read or Write cycle or an address within a Block for the Block Erase command. The Flash Linear Address must fall within a region for which BIOS has access permissions. Hardware must convert the FLA into a Flash Physical Address (FPA) before running this cycle on the SPI bus.

15.1.5 FDATA0—Flash Data 0 Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 10h
Attribute: R/W
Default Value: 00000000h
Size: 32 bits

Bit	Description
31:0	**Flash Data 0 (FD0)** — R/W. This field is shifted out as the SPI Data on the Master-Out Slave-In Data pin during the data portion of the SPI cycle. This register also shifts in the data from the Master-In Slave-Out pin into this register during the data portion of the SPI cycle. The data is always shifted starting with the least significant byte, msb to lsb, followed by the next least significant byte, msb to lsb, and so on. Specifically, the shift order on SPI in terms of bits within this register is: 7-6-5-4-3-2-1-0-15-14-13-…8-23-22-…16-31…24 Bit 24 is the last bit shifted out/in. There are no alignment assumptions; byte 0 always represents the value specified by the cycle address. The data in this register may be modified by the hardware during any programmed SPI transaction. Direct Memory Reads do not modify the contents of this register.

15.1.6 FDATAN—Flash Data [N] Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 14h, SPIBAR + 18h, SPIBAR + 1Ch, SPIBAR + 20h, SPIBAR + 24h, SPIBAR + 28h, SPIBAR + 2Ch, SPIBAR + 30h, SPIBAR + 34h, SPIBAR + 38h, SPIBAR + 3Ch, SPIBAR + 40h, SPIBAR + 44h, SPIBAR + 48h, SPIBAR + 4Ch
Attribute: R/W
Default Value: 00000000h
Size: 32 bits

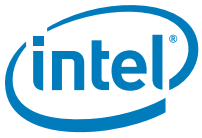
Bit	Description
31:0	**Flash Data N (FD[N])** — R/W. Similar definition as Flash Data 0. However, this register does not begin shifting until FD[N-1] has completely shifted in/out.

15.1.7 FRAP—Flash Regions Access Permissions Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 50h
Attribute: RO, R/W
Default Value: 00000202h
Size: 32 bits

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

Bit	Description
31:24	**BIOS Master Write Access Grant (BMWAG)** — R/W. Each bit [31:29] corresponds to Master[7:0]. BIOS can grant one or more masters write access to the BIOS region 1 overriding the permissions in the Flash Descriptor. Master[1] is Host processor/BIOS, Master[2] is Intel® Management Engine, Master[3] is Host processor/GbE. Master[0] and Master[7:4] are reserved. The contents of this register are locked by the FLOCKDN bit.



Bit	Description
23:16	**BIOS Master Read Access Grant (BMRAG) —** R/W. Each bit [28:16] corresponds to Master[7:0]. BIOS can grant one or more masters read access to the BIOS region 1 overriding the read permissions in the Flash Descriptor. Master[1] is Host processor/BIOS, Master[2] is Intel® Management Engine, Master[3] is Host processor/GbE. Master[0] and Master[7:4] are reserved. The contents of this register are locked by the FLOCKDN bit
15:8	**BIOS Region Write Access (BRWA) —** RO. Each bit [15:8] corresponds to Regions [7:0]. If the bit is set, this master can erase and write that particular region through register accesses. The contents of this register are that of the Flash Descriptor. Flash Master 1 Master Region Write Access OR a particular master has granted BIOS write permissions in their Master Write Access Grant register or the Flash Descriptor Security Override strap is set.
7:0	**BIOS Region Read Access (BRRA)** — RO. Each bit [7:0] corresponds to Regions [7:0]. If the bit is set, this master can read that particular region through register accesses. The contents of this register are that of the Flash Descriptor.Flash Master 1.Master Region Write Access OR a particular master has granted BIOS read permissions in their Master Read Access Grant register or the Flash Descriptor Security Override strap is set.

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

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

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

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

15.1.9 FREG1—Flash Region 1 (BIOS Descriptor) Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 58h Attribute: RO
Default Value: 00000000h Size: 32 bits

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

Bit	Description
31:29	Reserved
28:16	**Region Limit (RL) —** RO. This specifies address bits 24:12 for the Region 1 Limit. The value in this register is loaded from the contents in the Flash Descriptor.FLREG1.Region Limit.
15:13	Reserved
12:0	**Region Base (RB)** — RO. This specifies address bits 24:12 for the Region 1 Base The value in this register is loaded from the contents in the Flash Descriptor.FLREG1.Region Base.

15.1.10 FREG2—Flash Region 2 (Intel® ME) Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 5Ch Attribute: RO
Default Value: 00000000h Size: 32 bits

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

Bit	Description
31:29	Reserved
28:16	**Region Limit (RL) —** RO. This specifies address bits 24:12 for the Region 2 Limit. The value in this register is loaded from the contents in the Flash Descriptor.FLREG2.Region Limit.
15:13	Reserved
12:0	**Region Base (RB)** — RO. This specifies address bits 24:12 for the Region 2 Base The value in this register is loaded from the contents in the Flash Descriptor.FLREG2.Region Base

15.1.11 FREG3—Flash Region 3 (GbE) Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 60h Attribute: RO
Default Value: 00000000h Size: 32 bits

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

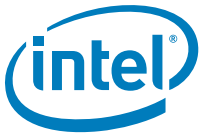
Bit	Description
31:29	Reserved
28:16	**Region Limit (RL) —** RO. This specifies address bits 24:12 for the Region 3 Limit. The value in this register is loaded from the contents in the Flash Descriptor.FLREG3.Region Limit.
15:13	Reserved
12:0	**Region Base (RB)** — RO. This specifies address bits 24:12 for the Region 3 Base The value in this register is loaded from the contents in the Flash Descriptor.FLREG3.Region Base

15.1.12 FREG4—Flash Region 4 (Platform Data) Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 64h Attribute: RO
Default Value: 00000000h Size: 32 bits

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

Bit	Description
31:29	Reserved
28:16	**Region Limit (RL) —** RO. This specifies address bits 24:12 for the Region 4 Limit. The value in this register is loaded from the contents in the Flash Descriptor.FLREG4.Region Limit.
15:13	Reserved
12:0	**Region Base (RB)** — RO. This specifies address bits 24:12 for the Region 4 Base The value in this register is loaded from the contents in the Flash Descriptor.FLREG4.Region Base.



15.1.13 PR0—Protected Range 0 Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 74h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits

Note: This register can not be written when the FLOCKDN bit is set to 1.

Bit	Description
31	**Write Protection Enable** — R/W. When set, this bit indicates that the Base and Limit fields in this register are valid and that writes and erases directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared.
30:29	Reserved
28:16	**Protected Range Limit —** R/W. This field corresponds to FLA address bits 24:12 and specifies the upper limit of the protected range. Address bits 11:0 are assumed to be FFFh for the limit comparison. Any address greater than the value programmed in this field is unaffected by this protected range.
15	**Read Protection Enable** — R/W. When set, this bit indicates that the Base and Limit fields in this register are valid and that read directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared.
14:13	Reserved
12:0	**Protected Range Base** — R/W. This field corresponds to FLA address bits 24:12 and specifies the lower base of the protected range. Address bits 11:0 are assumed to be 000h for the base comparison. Any address less than the value programmed in this field is unaffected by this protected range.

15.1.14 PR1—Protected Range 1 Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 78h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits

Note: This register can not be written when the FLOCKDN bit is set to 1.

Bit	Description
31	**Write Protection Enable** — R/W. When set, this bit indicates that the Base and Limit fields in this register are valid and that writes and erases directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared.
30:29	Reserved
28:16	**Protected Range Limit —** R/W. This field corresponds to FLA address bits 24:12 and specifies the upper limit of the protected range. Address bits 11:0 are assumed to be FFFh for the limit comparison. Any address greater than the value programmed in this field is unaffected by this protected range.
15	**Read Protection Enable** — R/W. When set, this bit indicates that the Base and Limit fields in this register are valid and that read directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared.
14:13	Reserved
12:0	**Protected Range Base** — R/W. This field corresponds to FLA address bits 24:12 and specifies the lower base of the protected range. Address bits 11:0 are assumed to be 000h for the base comparison. Any address less than the value programmed in this field is unaffected by this protected range.

15.1.15 PR2—Protected Range 2 Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 7Ch
Default Value: 00000000h
Attribute: R/W
Size: 32 bits

Note: This register can not be written when the FLOCKDN bit is set to 1.

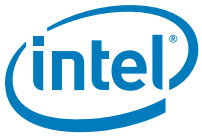
Bit	Description
31	**Write Protection Enable** — R/W. When set, this bit indicates that the Base and Limit fields in this register are valid and that writes and erases directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared.
30:29	Reserved
28:16	**Protected Range Limit —** R/W. This field corresponds to FLA address bits 24:12 and specifies the upper limit of the protected range. Address bits 11:0 are assumed to be FFFh for the limit comparison. Any address greater than the value programmed in this field is unaffected by this protected range.
15	**Read Protection Enable** — R/W. When set, this bit indicates that the Base and Limit fields in this register are valid and that read directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared.
14:13	Reserved
12:0	**Protected Range Base** — R/W. This field corresponds to FLA address bits 24:12 and specifies the lower base of the protected range. Address bits 11:0 are assumed to be 000h for the base comparison. Any address less than the value programmed in this field is unaffected by this protected range.

15.1.16 PR3—Protected Range 3 Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 80h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits

Note: This register can not be written when the FLOCKDN bit is set to 1.

Bit	Description
31	**Write Protection Enable** — R/W. When set, this bit indicates that the Base and Limit fields in this register are valid and that writes and erases directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared.
30:29	Reserved
28:16	**Protected Range Limit —** R/W. This field corresponds to FLA address bits 24:12 and specifies the upper limit of the protected range. Address bits 11:0 are assumed to be FFFh for the limit comparison. Any address greater than the value programmed in this field is unaffected by this protected range.
15	**Read Protection Enable** — R/W. When set, this bit indicates that the Base and Limit fields in this register are valid and that read directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared.
14:13	Reserved
12:0	**Protected Range Base** — R/W. This field corresponds to FLA address bits 24:12 and specifies the lower base of the protected range. Address bits 11:0 are assumed to be 000h for the base comparison. Any address less than the value programmed in this field is unaffected by this protected range.



15.1.17 PR4—Protected Range 4 Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 84h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits

Note: This register can not be written when the FLOCKDN bit is set to 1.

Bit	Description
31	**Write Protection Enable** — R/W. When set, this bit indicates that the Base and Limit fields in this register are valid and that writes and erases directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared.
30:29	Reserved
28:16	**Protected Range Limit —** R/W. This field corresponds to FLA address bits 24:12 and specifies the upper limit of the protected range. Address bits 11:0 are assumed to be FFFh for the limit comparison. Any address greater than the value programmed in this field is unaffected by this protected range.
15	**Read Protection Enable** — R/W. When set, this bit indicates that the Base and Limit fields in this register are valid and that read directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared.
14:13	Reserved
12:0	**Protected Range Base** — R/W. This field corresponds to FLA address bits 24:12 and specifies the lower base of the protected range. Address bits 11:0 are assumed to be 000h for the base comparison. Any address less than the value programmed in this field is unaffected by this protected range.

15.1.18 SSFS—Software Sequencing Flash Status Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 90h
Default Value: 00h
Attribute: RO, R/WC
Size: 8 bits

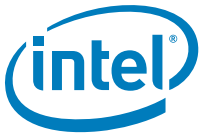
Note: The Software Sequencing control and status registers are reserved if the hardware sequencing control and status registers are used.

Bit	Description
7:5	Reserved
4	**Access Error Log (AEL) —** RO. This bit reflects the value of the Hardware Sequencing Status AEL register.
3	**Flash Cycle Error (FCERR) —** R/WC. Hardware sets this bit to 1 when a programmed access is blocked from running on the SPI interface due to one of the protection policies or when any of the programmed cycle registers is written while a programmed access is already in progress. This bit remains asserted until cleared by software writing a 1 or hardware reset due to a global reset or host partition reset in an Intel ME enabled system.
2	**Cycle Done Status** — R/WC. Intel® Xeon® Processor D-1500 Product Family sets this bit to 1 when the SPI Cycle completes (that is, SCIP bit is 0) after software sets the GO bit. This bit remains asserted until cleared by software writing a 1 or hardware reset due to a global reset or host partition reset in an Intel® ME enabled system. When this bit is set and the SPI SMI# Enable bit is set, an internal signal is asserted to the SMI# generation block. Software must make sure this bit is cleared prior to enabling the SPI SMI# assertion for a new programmed access.
1	Reserved
0	**SPI Cycle In Progress (SCIP)** — RO. Hardware sets this bit when software sets the SPI Cycle Go bit in the Command register. This bit remains set until the cycle completes on the SPI interface. Hardware automatically sets and clears this bit so that software can determine when read data is valid and/or when it is safe to begin programming the next command. Software must only program the next command when this bit is 0.

15.1.19 SSFC—Software Sequencing Flash Control Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 91h Attribute: R/W
Default Value: F80000h Size: 24 bits

Bit	Description
23:19	Reserved – BIOS must set this field to `11111'b
18:16	**SPI Cycle Frequency (SCF) —** R/W. This register sets frequency to use for all SPI software sequencing cycles (write, erase, fast read, read status, and so on) except for the read cycle which always run at 20 MHz. 000 = 20 MHz 001 = 33 MHz 100 = 50 MHz All other values reserved. This register is locked when the SPI Configuration Lock-Down bit is set.
15	**SPI SMI# Enable (SME)** — R/W. When set to 1, the SPI asserts an SMI# request whenever the Cycle Done Status bit is 1.
14	**Data Cycle (DS)** — R/W. When set to 1, there is data that corresponds to this transaction. When 0, no data is delivered for this cycle, and the dBC and data fields themselves are don't cares.
13:8	**Data Byte Count (dBC)** — R/W. This field specifies the number of bytes to shift in or out during the data portion of the SPI cycle. The valid settings (in decimal) are any value from 0 to 63. The number of bytes transferred is the value of this field plus 1. When this field is 00_0000b, there is 1 byte to transfer and that 11_1111b means there are 64 bytes to transfer.
7	Reserved
6:4	**Cycle Opcode Pointer (COP)** — R/W. This field selects one of the programmed opcodes in the Opcode Menu to be used as the SPI Command/Opcode. In the case of an Atomic Cycle Sequence, this determines the second command.
3	**Sequence Prefix Opcode Pointer (SPOP)** — R/W. This field selects one of the two programmed prefix opcodes for use when performing an Atomic Cycle Sequence. A value of 0 points to the opcode in the least significant byte of the Prefix Opcodes register. By making this programmable, Intel® Xeon® Processor D-1500 Product Family supports flash devices that have different opcodes for enabling writes to the data space versus status register.
2	**Atomic Cycle Sequence (ACS)** — R/W. When set to 1 along with the SCGO assertion, Intel® Xeon® Processor D-1500 Product Family will execute a sequence of commands on the SPI interface without allowing the LAN component to arbitrate and interleave cycles. The sequence is composed of: • Atomic Sequence Prefix Command (8-bit opcode only) • Primary Command specified below by software (can include address and data) • Polling the Flash Status Register (opcode 05h) until bit 0 becomes 0b. The SPI Cycle in Progress bit remains set and the Cycle Done Status bit remains unset until the Busy bit in the Flash Status Register returns 0.
1	**SPI Cycle Go (SCGO)** — R/WS. This bit always returns 0 on reads. However, a write to this register with a 1 in this bit starts the SPI cycle defined by the other bits of this register. The "SPI Cycle in Progress" (SCIP) bit gets set by this action. Hardware must ignore writes to this bit while the Cycle In Progress bit is set. Hardware allows other bits in this register to be programmed for the same transaction when writing this bit to 1. This saves an additional memory write.
0	Reserved



15.1.20 PREOP—Prefix Opcode Configuration Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 94h Attribute: R/W
Default Value: 0000h Size: 16 bits

Bit	Description
15:8	**Prefix Opcode 1**— R/W. Software programs an SPI opcode into this field that is permitted to run as the first command in an atomic cycle sequence.
7:0	**Prefix Opcode 0** — R/W. Software programs an SPI opcode into this field that is permitted to run as the first command in an atomic cycle sequence.

Note: This register is not writable when the Flash Configuration Lock-Down bit (SPIBAR + 04h:15) is set.

15.1.21 OPTYPE—Opcode Type Configuration Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 96h Attribute: R/W
Default Value: 0000h Size: 16 bits

Entries in this register correspond to the entries in the Opcode Menu Configuration register.

Note: The definition below only provides write protection for opcodes that have addresses associated with them. Therefore, any erase or write opcodes that do not use an address should be avoided (for example, "Chip Erase" and "Auto-Address Increment Byte Program")

Bit	Description
15:14	**Opcode Type 7** — R/W. See the description for bits 1:0
13:12	**Opcode Type 6** — R/W. See the description for bits 1:0
11:10	**Opcode Type 5** — R/W. See the description for bits 1:0
9:8	**Opcode Type 4** — R/W. See the description for bits 1:0
7:6	**Opcode Type 3** — R/W. See the description for bits 1:0
5:4	**Opcode Type 2** — R/W. See the description for bits 1:0
3:2	**Opcode Type 1** — R/W. See the description for bits 1:0
1:0	**Opcode Type 0** — R/W. This field specifies information about the corresponding Opcode 0. This information allows the hardware to 1) know whether to use the address field and 2) provide BIOS and Shared Flash protection capabilities. The encoding of the two bits is: 00 = No address associated with this Opcode; Read cycle type 01 = No address associated with this Opcode; Write cycle type 10 = Address required; Read cycle type 11 = Address required; Write cycle type

Note: This register is not writable when the SPI Configuration Lock-Down bit (SPIBAR + 00h:15) is set.

15.1.22 OPMENU—Opcode Menu Configuration Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + 98h Attribute: R/W

Default Value: 0000000000000000h Size: 64 bits

Eight entries are available in this register to give BIOS a sufficient set of commands for communicating with the flash device, while also restricting what malicious software can do. This keeps the hardware flexible enough to operate with a wide variety of SPI devices.

Note: It is recommended that BIOS avoid programming Write Enable opcodes in this menu. Malicious software could then perform writes and erases to the SPI flash without using the atomic cycle mechanism. This could cause functional failures in a shared flash environment. Write Enable opcodes should only be programmed in the Prefix Opcodes.

Bit	Description
63:56	**Allowable Opcode 7** — R/W. See the description for bits 7:0
55:48	**Allowable Opcode 6** — R/W. See the description for bits 7:0
47:40	**Allowable Opcode 5** — R/W. See the description for bits 7:0
39:32	**Allowable Opcode 4** — R/W. See the description for bits 7:0
31:24	**Allowable Opcode 3** — R/W. See the description for bits 7:0
23:16	**Allowable Opcode 2** — R/W. See the description for bits 7:0
15:8	**Allowable Opcode 1** — R/W. See the description for bits 7:0
7:0	**Allowable Opcode 0** — R/W. Software programs an SPI opcode into this field for use when initiating SPI commands through the Control Register.

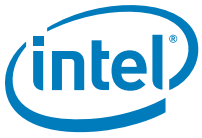
This register is not writable when the SPI Configuration Lock-Down bit (SPIBAR + 00h:15) is set.

15.1.23 BBAR—BIOS Base Address Configuration Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + A0h Attribute: R/W, RO
Default Value: 00000000h Size: 32 bits

Eight entries are available in this register to give BIOS a sufficient set of commands for communicating with the flash device, while also restricting what malicious software can do. This keeps the hardware flexible enough to operate with a wide variety of SPI devices.

Bit	Description
31:24	Reserved
23:8	**Bottom of System Flash**— R/W. This field determines the bottom of the System BIOS. Intel® Xeon® Processor D-1500 Product Family will not run programmed commands nor memory reads whose address field is less than this value. this field corresponds to bits 23:8 of the 3-byte address; bits 7:0 are assumed to be 00h for this vector when comparing to a potential SPI address. ***Note:*** The SPI host controller prevents any programmed cycle using the address register with an address less than the value in this register. Some flash devices specify that the Read ID command must have an address of 0000h or 0001h. If this command must be supported with these devices, it must be performed with the BIOS BAR.
7:0	Reserved



15.1.24 FDOC—Flash Descriptor Observability Control Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + B0h | Attribute: R/W
Default Value: 00000000h | Size: 32 bits

Note: This register that can be used to observe the contents of the Flash Descriptor that is stored in Intel® Xeon® Processor D-1500 Product Family Flash Controller. This register is only applicable when SPI device is in descriptor mode.

Bit	Description
31:15	Reserved
14:12	**Flash Descriptor Section Select (FDSS)** — R/W. Selects which section within the loaded Flash Descriptor to observe. 000 = Flash Signature and Descriptor Map 001 = Component 010 = Region 011 = Master 111 = Reserved
11:2	**Flash Descriptor Section Index (FDSI) —** R/W. Selects the DW offset within the Flash Descriptor Section to observe.
1:0	Reserved

15.1.25 FDOD—Flash Descriptor Observability Data Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + B4h | Attribute: RO
Default Value: 00000000h | Size: 32 bits

Note: This register that can be used to observe the contents of the Flash Descriptor that is stored in Intel® Xeon® Processor D-1500 Product Family Flash Controller.

Bit	Description
31:0	**Flash Descriptor Section Data (FDSD) —** RO. Returns the DW of data to observe as selected in the Flash Descriptor Observability Control.

15.1.26 AFC—Additional Flash Control Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + C0h | Attribute: RO, R/W
Default Value: 00000000h | Size: 32 bits.

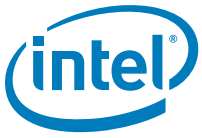
Bit	Description
31:3	Reserved
2:1	**Flash Controller Interface Dynamic Clock Gating Enable** — R/W. 0 = Flash Controller Interface Dynamic Clock Gating is Disabled 1 = Flash Controller Interface Dynamic Clock Gating is Enabled Other configurations are Reserved.
0	**Flash Controller Core Dynamic Clock Gating Enable** — R/W. 0 = Flash Controller Core Dynamic Clock Gating is Disabled 1 = Flash Controller Core Dynamic Clock Gating is Enabled

15.1.27 LVSCC— Host Lower Vendor Specific Component Capabilities Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + C4h
Default Value: 00000000h
Attribute: RO, R/WL
Size: 32 bits

Note: All attributes described in LVSCC must apply to all flash space below the FPBA, even if it spans between two separate flash parts. This register is only applicable when SPI device is in descriptor mode.

Bit	Description
31:24	Reserved
23	**Vendor Component Lock (LVCL)** — R/W. This register locks itself when set. 0 = The lock bit is not set 1 = The Vendor Component Lock bit is set. ***Note:*** This bit applies to both UVSCC and LVSCC registers.
22:16	Reserved
15:8	**Lower Erase Opcode (LEO)**— R/W. This register is programmed with the Flash erase instruction opcode required by the vendor's Flash component. This register is locked by the Vendor Component Lock (LVCL) bit.
7:5	Reserved
4	**Write Enable on Write Status (LWEWS)** — R/W. This register is locked by the Vendor Component Lock (LVCL) bit. 0 = No automatic write of 00h will be made to the SPI flash's status register) 1 = A write of 00h to the SPI flash's status register will be sent on EVERY write and erase to the SPI flash. 06h 01h 00h is the opcode sequence used to unlock the Status register. ***Notes:*** 1. This bit should not be set to 1 if there are non-volatile bits in the SPI flash's status register. This may lead to premature flash wear out. 2. This is not an atomic sequence. If the SPI component's status register is non-volatile, then BIOS should issue an atomic software sequence cycle to unlock the flash part. 3. Bit 3 and bit 4 should NOT be both set to 1.
3	**Lower Write Status Required (LWSR)** — R/W. This register is locked by the Vendor Component Lock (LVCL) bit. 0 = No automatic write of 00h will be made to the SPI flash's status register) 1 = A write of 00h to the SPI flash's status register will be sent on EVERY write and erase to the SPI flash. 50h 01h 00h is the opcode sequence used to unlock the Status register. ***Notes:*** 1. This bit should not be set to 1 if there are non volatile bits in the SPI flash's status register. This may lead to premature flash wear out. 2. This is not an atomic sequence. If the SPI component's status register is non-volatile, then BIOS should issue an atomic software sequence cycle to unlock the flash part. 3. Bit 3 and bit 4 should NOT be both set to 1.
2	**Lower Write Granularity (LWG) —** R/W**.** This register is locked by the Vendor Component Lock (LVCL) bit. 0 = 1 Byte 1 = 64 Byte ***Notes:*** 1. If more than one Flash component exists, this field must be set to the lowest common write granularity of the different Flash components. 2. If using 64 B write, BIOS must ensure that multiple byte writes do not occur over 256 B boundaries. This will lead to corruption as the write will wrap around the page boundary on the SPI flash part. This is a a feature page writable SPI flash.
1:0	**Lower Block/Sector Erase Size (LBES)—** R/W. This field identifies the erasable sector size for all Flash components. 00 = 256 Byte 01 = 4 KB 10 = 8 KB 11 = 64 KB This register is locked by the Vendor Component Lock (LVCL) bit. Hardware takes no action based on the value of this register. The contents of this register are to be used only by software and can be read in the HSFSTS.BERASE register in both the BIOS and the GbE program registers if FLA is less than FPBA.



15.1.28 UVSCC— Host Upper Vendor Specific Component Capabilities Register (SPI Memory Mapped Configuration Registers)

Memory Address:	SPIBAR + C8h	Attribute:	RO, R/WL
Default Value:	00000000h	Size:	32 bits

Note: All attributes described in UVSCC must apply to all flash space equal to or above the FPBA, even if it spans between two separate flash parts. This register is only applicable when SPI device is in descriptor mode.

Note: To prevent this register from being modified you must use LVSCC.VCL bit.

Bit	Description
31:16	Reserved
15:8	**Upper Erase Opcode (UEO)**— R/W. This register is programmed with the Flash erase instruction opcode required by the vendor's Flash component. This register is locked by the Vendor Component Lock (UVCL) bit.
7:5	Reserved
4	**Write Enable on Write Status (UWEWS)** — R/W. This register is locked by the Vendor Component Lock (UVCL) bit. 0 = No automatic write of 00h will be made to the SPI flash's status register) 1 = A write of 00h to the SPI flash's status register will be sent on EVERY write and erase to the SPI flash. 06h 01h 00h is the opcode sequence used to unlock the Status register. ***Notes:*** 1. This bit should not be set to 1 if there are non volatile bits in the SPI flash's status register. This may lead to premature flash wear out. 2. This is not an atomic sequence. If the SPI component's status register is non-volatile, then BIOS should issue an atomic software sequence cycle to unlock the flash part. 3. Bit 3 and bit 4 should NOT be both set to 1.
3	**Upper Write Status Required (UWSR)** — R/W. This register is locked by the Vendor Component Lock (UVCL) bit. 0 = No automatic write of 00h will be made to the SPI flash's status register) 1 = A write of 00h to the SPI flash's status register will be sent on EVERY write and erase to the SPI flash. 50h 01h 00h is the opcode sequence used to unlock the Status register. ***Notes:*** 1. This bit should not be set to '1' if there are non volatile bits in the SPI flash's status register. This may lead to premature flash wear out. 2. This is not an atomic sequence. If the SPI component's status register is non-volatile, then BIOS should issue an atomic software sequence cycle to unlock the flash part. 3. Bit 3 and bit 4 should NOT be both set to 1.
2	**Upper Write Granularity (UWG) —** R/W. This register is locked by the Vendor Component Lock (UVCL) bit. 0 = 1 Byte 1 = 64 Byte ***Notes:*** 1. If more than one Flash component exists, this field must be set to the lowest common write granularity of the different Flash components. 2. If using 64 B write, BIOS must ensure that multiple byte writes do not occur over 256 B boundaries. This will lead to corruption as the write will wrap around the page boundary on the SPI flash part. This is a a feature page writable SPI flash.

Bit	Description
1:0	**Upper Block/Sector Erase Size (UBES)—** R/W. This field identifies the erasable sector size for all Flash components. Valid Bit Settings: 00 = 256 Byte 01 = 4 KB 10 = 8 KB 11 = 64 KB This register is locked by the Vendor Component Lock (UVCL) bit. Hardware takes no action based on the value of this register. The contents of this register are to be used only by software and can be read in the HSFSTS.BERASE register in both the BIOS and the GbE program registers if FLA is greater or equal to FPBA.

15.1.29 FPB—Flash Partition Boundary Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + D0h Attribute: RO
Default Value: 00000000h Size: 32 bits

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

Bit	Description
31:13	Reserved
12:0	**Flash Partition Boundary Address (FPBA)** — RO. This register reflects the value of Flash Descriptor Component FPBA field.

15.1.30 SRDL—Soft Reset Data Lock Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + F0h Attribute: R/WL
Default Value: 00000000h Size: 32 bits

Bit	Description
31:1	Reserved
0	**Set_Stap Lock (SSL)** — R/WL. 0 = The SRDL (this register), SRDC (SPIBAR+F4h), and SRD (SPIBAR+F4h) registers are writeable. 1 = The SRDL (this register), SRDC (SPIBAR+F4h), and SRD (SPIBAR+F4h) registers are locked. ***Note:*** That this bit is reset to '0' on CF9h resets.

15.1.31 SRDC—Soft Reset Data Control Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + F4h Attribute: R/WL
Default Value: 00000000h Size: 32 bits

Bit	Description
31:1	Reserved
0	**Soft Reset Data Select (SRDS)** — R/WL. 0 = The Set_Strap data sends the default processor configuration data. 1 = The Set_Strap message bits come from the Set_Strap Msg Data register. ***Notes:*** 1. This bit is reset by the RSMRST# or when the Resume well loses power. 2. This bit is locked by the SSL bit (SPIBAR+F0h:bit 0).

15.1.32 SRD—Soft Reset Data Register (SPI Memory Mapped Configuration Registers)

Memory Address: SPIBAR + F8h Attribute: R/WL
Default Value: 00000000h Size: 32 bits

Bit	Description
31:14	Reserved
13:0	**Set_Stap Data (SSD)** — R/WL. ***Notes:*** 1. These bits are reset by the RSMRST#, or when the Resume well loses power. 2. These bits are locked by the SSL bit (SPIBAR+F0h:bit 0).

15.2 Flash Descriptor Records

The following sections describe the data structure of the Flash Descriptor on the SPI device. These are not registers within Intel® Xeon® Processor D-1500 Product Family.

15.3 OEM Section

Memory Address: F00h
Default Value: Size: 256 Bytes

256 Bytes are reserved at the top of the Flash Descriptor for use by the OEM. The information stored by the OEM can only be written during the manufacturing process as the Flash Descriptor read/write permissions must be set to Read Only when the computer leaves the manufacturing floor. Intel® Xeon® Processor D-1500 Product Family Flash controller does not read this information. FFh is suggested to reduce programming time.

15.4 GbE SPI Flash Program Registers

The GbE Flash registers are memory-mapped with a base address MBARB found in the GbE LAN register chapter Device 25: Function 0: Offset 14h. The individual registers are then accessible at MBARB + Offset as indicated in the following table.

These memory mapped registers must be accessed in byte, word, or DWord quantities.

Note: These register are only applicable when SPI flash is used in descriptor mode.

Table 15-2. Gigabit LAN SPI Flash Program Register Address Map (GbE LAN Memory Mapped Configuration Registers) (Sheet 1 of 2)

MBARB + Offset	Mnemonic	Register Name	Default	Attribute
00h–03h	GLFPR	Gigabit LAN Flash Primary Region	00000000h	RO
04h–05h	HSFS	Hardware Sequencing Flash Status	0000h	RO, R/WC, R/W
06h–07h	HSFC	Hardware Sequencing Flash Control	0000h	R/W, R/WS
08h–0Bh	FADDR	Flash Address	00000000h	R/W
0Ch–0Fh	—	Reserved	00000000h	
10h–13h	FDATA0	Flash Data 0	00000000h	R/W
14h–4Fh	—	Reserved	00000000h	
50h–53h	FRAP	Flash Region Access Permissions	00000000h	RO, R/W

Table 15-2. Gigabit LAN SPI Flash Program Register Address Map (GbE LAN Memory Mapped Configuration Registers) (Sheet 2 of 2)

MBARB + Offset	Mnemonic	Register Name	Default	Attribute
54h–57h	FREG0	Flash Region 0	00000000h	RO
58h–5Bh	FREG1	Flash Region 1	00000000h	RO
5Ch–5F	FREG2	Flash Region 2	00000000h	RO
60h–63h	FREG3	Flash Region 3	00000000h	RO
64h–73h	—	Reserved for Future Flash Regions		
74h–77h	PR0	Flash Protected Range 0	00000000h	R/W
78h–7Bh	PR1	Flash Protected Range 1	00000000h	R/W
7Ch–8Fh	—	Reserved		
90h	SSFS	Software Sequencing Flash Status	00h	RO, R/WC
91h–93h	SSFC	Software Sequencing Flash Control	000000h	R/W
94h–95h	PREOP	Prefix Opcode Configuration	0000h	R/W
96h–97h	OPTYPE	Opcode Type Configuration	0000h	R/W
98h–9Fh	OPMENU	Opcode Menu Configuration	0000000000000000h	R/W
A0h–DFh	—	Reserved		

15.4.1 GLFPR –Gigabit LAN Flash Primary Region Register (GbE LAN Memory Mapped Configuration Registers)

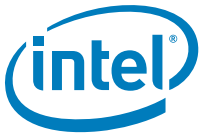
Memory Address: MBARB + 00h Attribute: RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:29	Reserved
28:16	**GbE Flash Primary Region Limit (PRL)—** RO. This specifies address bits 24:12 for the Primary Region Limit. The value in this register loaded from the contents in the Flash Descriptor.FLREG3.Region Limit
15:13	Reserved
12:0	**GbE Flash Primary Region Base (PRB)** — RO. This specifies address bits 24:12 for the Primary Region Base The value in this register is loaded from the contents in the Flash Descriptor.FLREG3.Region Base

15.4.2 HSFS—Hardware Sequencing Flash Status Register (GbE LAN Memory Mapped Configuration Registers)

Memory Address: MBARB + 04h Attribute: RO, R/WC, R/W
Default Value: 0000h Size: 16 bits

Bit	Description
15	**Flash Configuration Lock-Down (FLOCKDN)**— R/W. When set to 1, those Flash Program Registers that are locked down by this FLOCKDN bit cannot be written. Once set to 1, this bit can only be cleared by a hardware reset due to a global reset or host partition reset in an Intel® ME enabled system.
14	**Flash Descriptor Valid (FDV)—** RO. This bit is set to a 1 if the Flash Controller read the correct Flash Descriptor Signature. If the Flash Descriptor Valid bit is not 1, software cannot use the Hardware Sequencing registers, but must use the software sequencing registers. Any attempt to use the Hardware Sequencing registers will result in the FCERR bit being set.



Bit	Description
13	**Flash Descriptor Override Pin Strap Status (FDOPSS)—** RO. This bit indicates the condition of the Flash Descriptor Security Override / Intel ME Debug Mode pin strap. 0 = The Flash Descriptor Security Override / Intel ME Debug Mode strap is set using external pull-up on MFG_MODE_STRAP 1 = No override
12:6	Reserved
5	**SPI Cycle In Progress (SCIP)—** RO. Hardware sets this bit when software sets the Flash Cycle Go (FGO) bit in the Hardware Sequencing Flash Control register. This bit remains set until the cycle completes on the SPI interface. Hardware automatically sets and clears this bit so that software can determine when read data is valid and/or when it is safe to begin programming the next command. Software must only program the next command when this bit is 0.
4:3	**Block/Sector Erase Size (BERASE)** — RO. This field identifies the erasable sector size for all Flash components. 00 = 256 Byte 01 = 4 K Byte 10 = 8 K Byte 11 = 64 K Byte If the Flash Linear Address is less than FPBA then this field reflects the value in the LVSCC.LBES register. If the Flash Linear Address is greater or equal to FPBA then this field reflects the value in the UVSCC.UBES register.
2	**Access Error Log (AEL)**— R/W/C. Hardware sets this bit to a 1 when an attempt was made to access the BIOS region using the direct access method or an access to the BIOS Program Registers that violated the security restrictions. This bit is simply a log of an access security violation. This bit is cleared by software writing a 1.
1	**Flash Cycle Error (FCERR)** — R/W/C. Hardware sets this bit to 1 when an program register access is blocked to the FLASH due to one of the protection policies or when any of the programmed cycle registers is written while a programmed access is already in progress. This bit remains asserted until cleared by software writing a 1 or until hardware reset occurs due to a global reset or host partition reset in an Intel ME enabled system. Software must clear this bit before setting the FLASH Cycle GO bit in this register.
0	**Flash Cycle Done (FDONE)** — R/W/C. Intel® Xeon® Processor D-1500 Product Family sets this bit to 1 when the SPI Cycle completes after software previously set the FGO bit. This bit remains asserted until cleared by software writing a 1 or hardware reset due to a global reset or host partition reset in an Intel® ME enabled system. When this bit is set and the SPI SMI# Enable bit is set, an internal signal is asserted to the SMI# generation block. Software must make sure this bit is cleared prior to enabling the SPI SMI# assertion for a new programmed access.

15.4.3 HSFC—Hardware Sequencing Flash Control Register (GbE LAN Memory Mapped Configuration Registers)

Memory Address: MBARB + 06h Attribute: R/W, R/WS
Default Value: 0000h Size: 16 bits

Bit	Description
15:10	Reserved
9:8	**Flash Data Byte Count (FdBC) —** R/W. This field specifies the number of bytes to shift in or out during the data portion of the SPI cycle. The contents of this register are 0s based with 0b representing 1 byte and 11b representing 4 bytes. The number of bytes transferred is the value of this field plus 1. This field is ignored for the Block Erase command.
7:3	Reserved
2:1	**FLASH Cycle (FCYCLE)** — R/W. This field defines the Flash SPI cycle type generated to the FLASH when the FGO bit is set as defined below: 00 = Read (1 up to 4 bytes by setting FdBC) 01 = Reserved 10 = Write (1 up to 4 bytes by setting FdBC) 11 = Block Erase

Bit	Description
0	**Flash Cycle Go (FGO)** — R/W/S. A write to this register with a 1 in this bit initiates a request to the Flash SPI Arbiter to start a cycle. This register is cleared by hardware when the cycle is granted by the SPI arbiter to run the cycle on the SPI bus. When the cycle is complete, the FDONE bit is set. Software is forbidden to write to any register in the HSFLCTL register between the FGO bit getting set and the FDONE bit being cleared. Any attempt to violate this rule will be ignored by hardware. Hardware allows other bits in this register to be programmed for the same transaction when writing this bit to 1. This saves an additional memory write. This bit always returns 0 on reads.

15.4.4 FADDR—Flash Address Register (GbE LAN Memory Mapped Configuration Registers)

Memory Address: MBARB + 08h Attribute: R/W
Default Value: 00000000h Size: 32 bits

Bit	Description
31:25	Reserved
24:0	**Flash Linear Address (FLA) —** R/W. The FLA is the starting byte linear address of a SPI Read or Write cycle or an address within a Block for the Block Erase command. The Flash Linear Address must fall within a region for which BIOS has access permissions.

15.4.5 FDATA0—Flash Data 0 Register (GbE LAN Memory Mapped Configuration Registers)

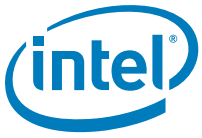
Memory Address: MBARB + 10h Attribute: R/W
Default Value: 00000000h Size: 32 bits

Bit	Description
31:0	**Flash Data 0 (FD0)** — R/W. This field is shifted out as the SPI Data on the Master-Out Slave-In Data pin during the data portion of the SPI cycle. This register also shifts in the data from the Master-In Slave-Out pin into this register during the data portion of the SPI cycle. The data is always shifted starting with the least significant byte, msb to lsb, followed by the next least significant byte, msb to lsb, and so on. Specifically, the shift order on SPI in terms of bits within this register is: 7-6-5-4-3-2-1-0-15-14-13-…8-23-22-…16-31…24 Bit 24 is the last bit shifted out/in. There are no alignment assumptions; byte 0 always represents the value specified by the cycle address. The data in this register may be modified by the hardware during any programmed SPI transaction. Direct Memory Reads do not modify the contents of this register.

15.4.6 FRAP—Flash Regions Access Permissions Register (GbE LAN Memory Mapped Configuration Registers)

Memory Address: MBARB + 50h Attribute: RO, R/W
Default Value: 00000808h Size: 32 bits

Bit	Description
31:28	Reserved
27:25	**GbE Master Write Access Grant (GMWAG)** — R/W. Each bit 27:25 corresponds to Master[3:1]. GbE can grant one or more masters write access to the GbE region 3 overriding the permissions in the Flash Descriptor. Master[1] is Host Processor/BIOS, Master[2] is Intel Management Engine, Master[3] is Host processor/GbE. The contents of this register are locked by the FLOCKDN bit.
24:20	Reserved



Bit	Description
19:17	**GbE Master Read Access Grant (GMRAG) —** R/W. Each bit 19:17 corresponds to Master[3:1]. GbE can grant one or more masters read access to the GbE region 3 overriding the read permissions in the Flash Descriptor. Master[1] is Host processor/BIOS, Master[2] is Intel® Management Engine, Master[3] is GbE. The contents of this register are locked by the FLOCKDN bit
16:12	Reserved
11:8	**GbE Region Write Access (GRWA) —** RO. Each bit 11:8 corresponds to Regions 3:0. If the bit is set, this master can erase and write that particular region through register accesses. The contents of this register are that of the Flash Descriptor. Flash Master 3.Master Region Write Access OR a particular master has granted GbE write permissions in their Master Write Access Grant register OR the Flash Descriptor Security Override strap is set.
7:4	Reserved
3:0	**GbE Region Read Access (GRRA)** — RO. Each bit 3:0 corresponds to Regions 3:0. If the bit is set, this master can read that particular region through register accesses. The contents of this register are that of the Flash Descriptor. Flash Master 3.Master Region Write Access OR a particular master has granted GbE read permissions in their Master Read Access Grant register.

15.4.7 FREG0—Flash Region 0 (Flash Descriptor) Register (GbE LAN Memory Mapped Configuration Registers)

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

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

15.4.8 FREG1—Flash Region 1 (BIOS Descriptor) Register (GbE LAN Memory Mapped Configuration Registers)

Memory Address: MBARB + 58h Attribute: RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:29	Reserved
28:16	**Region Limit (RL) —** RO. This specifies address bits 24:12 for the Region 1 Limit. The value in this register is loaded from the contents in the Flash Descriptor.FLREG1.Region Limit.
15:13	Reserved
12:0	**Region Base (RB)** — RO. This specifies address bits 24:12 for the Region 1 Base The value in this register is loaded from the contents in the Flash Descriptor.FLREG1.Region Base.

15.4.9 FREG2—Flash Region 2 (Intel® ME) Register (GbE LAN Memory Mapped Configuration Registers)

Memory Address: MBARB + 5Ch Attribute: RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:29	Reserved
28:16	**Region Limit (RL) —** RO. This specifies address bits 24:12 for the Region 2 Limit. The value in this register is loaded from the contents in the Flash Descriptor.FLREG2.Region Limit.
15:13	Reserved
12:0	**Region Base (RB)** — RO. This specifies address bits 24:12 for the Region 2 Base The value in this register is loaded from the contents in the Flash Descriptor.FLREG2.Region Base.

15.4.10 FREG3—Flash Region 3 (GbE) Register (GbE LAN Memory Mapped Configuration Registers)

Memory Address: MBARB + 60h Attribute: RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:29	Reserved
28:16	**Region Limit (RL) —** RO. This specifies address bits 24:12 for the Region 3 Limit. The value in this register is loaded from the contents in the Flash Descriptor.FLREG3.Region Limit.
15:13	Reserved
12:0	**Region Base (RB)** — RO. This specifies address bits 24:12 for the Region 3 Base The value in this register is loaded from the contents in the Flash Descriptor.FLREG3.Region Base.

15.4.11 PR0—Protected Range 0 Register (GbE LAN Memory Mapped Configuration Registers)

Memory Address: MBARB + 74h Attribute: R/W
Default Value: 00000000h Size: 32 bits

Note: This register can not be written when the FLOCKDN bit is set to 1.

Bit	Description
31	**Write Protection Enable** — R/W. When set, this bit indicates that the Base and Limit fields in this register are valid and that writes and erases directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared.
30:29	Reserved
28:16	**Protected Range Limit —** R/W. This field corresponds to FLA address bits 24:12 and specifies the upper limit of the protected range. Address bits 11:0 are assumed to be FFFh for the limit comparison. Any address greater than the value programmed in this field is unaffected by this protected range.
15	**Read Protection Enable** — R/W. When set, this bit indicates that the Base and Limit fields in this register are valid and that read directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared.
14:13	Reserved
12:0	**Protected Range Base** — R/W. This field corresponds to FLA address bits 24:12 and specifies the lower base of the protected range. Address bits 11:0 are assumed to be 000h for the base comparison. Any address less than the value programmed in this field is unaffected by this protected range.

15.4.12 PR1—Protected Range 1 Register (GbE LAN Memory Mapped Configuration Registers)

Memory Address: MBARB + 78h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits

Note: This register can not be written when the FLOCKDN bit is set to 1.

Bit	Description
31	**Write Protection Enable** — R/W. When set, this bit indicates that the Base and Limit fields in this register are valid and that writes and erases directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared.
30:29	Reserved
28:16	**Protected Range Limit —** R/W. This field corresponds to FLA address bits 24:12 and specifies the upper limit of the protected range. Address bits 11:0 are assumed to be FFFh for the limit comparison. Any address greater than the value programmed in this field is unaffected by this protected range.
15	**Read Protection Enable** — R/W. When set, this bit indicates that the Base and Limit fields in this register are valid and that read directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared.
14:13	Reserved
12:0	**Protected Range Base** — R/W. This field corresponds to FLA address bits 24:12 and specifies the lower base of the protected range. Address bits 11:0 are assumed to be 000h for the base comparison. Any address less than the value programmed in this field is unaffected by this protected range.

15.4.13 SSFS—Software Sequencing Flash Status Register (GbE LAN Memory Mapped Configuration Registers)

Memory Address: MBARB + 90h
Default Value: 00h
Attribute: RO, R/WC
Size: 8 bits

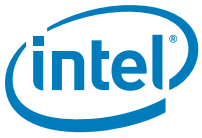
Note: The Software Sequencing control and status registers are reserved if the hardware sequencing control and status registers are used.

Bit	Description
7:5	Reserved
4	**Access Error Log (AEL) —** RO. This bit reflects the value of the Hardware Sequencing Status AEL register.
3	**Flash Cycle Error (FCERR) —** R/WC. Hardware sets this bit to 1 when a programmed access is blocked from running on the SPI interface due to one of the protection policies or when any of the programmed cycle registers is written while a programmed access is already in progress. This bit remains asserted until cleared by software writing a 1 or hardware reset due to a global reset or host partition reset in an Intel® ME enabled system.
2	**Cycle Done Status** — R/WC. Intel® Xeon® Processor D-1500 Product Family sets this bit to 1 when the SPI Cycle completes (that is, SCIP bit is 0) after software sets the GO bit. This bit remains asserted until cleared by software writing a 1 or hardware reset due to a global reset or host partition reset in an Intel® ME enabled system. When this bit is set and the SPI SMI# Enable bit is set, an internal signal is asserted to the SMI# generation block. Software must make sure this bit is cleared prior to enabling the SPI SMI# assertion for a new programmed access.
1	Reserved
0	**SPI Cycle In Progress (SCIP)** — RO. Hardware sets this bit when software sets the SPI Cycle Go bit in the Command register. This bit remains set until the cycle completes on the SPI interface. Hardware automatically sets and clears this bit so that software can determine when read data is valid and/or when it is safe to begin programming the next command. Software must only program the next command when this bit is 0.

15.4.14 SSFC—Software Sequencing Flash Control Register (GbE LAN Memory Mapped Configuration Registers)

Memory Address: MBARB + 91h Attribute: R/W
Default Value: 000000h Size: 24 bits

Bit	Description
23:19	Reserved
18:16	**SPI Cycle Frequency (SCF) —** R/W. This register sets frequency to use for all SPI software sequencing cycles (write, erase, fast read, read status, and so on) except for the read cycle which always run at 20 MHz. 000 = 20 MHz 001 = 33 MHz All other values = Reserved. This register is locked when the SPI Configuration Lock-Down bit is set.
15	Reserved
14	**Data Cycle (DS)** — R/W. When set to 1, there is data that corresponds to this transaction. When 0, no data is delivered for this cycle, and the dBC and data fields themselves are don't cares.
13:8	**Data Byte Count (dBC)** — R/W. This field specifies the number of bytes to shift in or out during the data portion of the SPI cycle. The valid settings (in decimal) are any value from 0 to 3. The number of bytes transferred is the value of this field plus 1. When this field is 00b, then there is 1 byte to transfer and that 11b means there are 4 bytes to transfer.
7	Reserved
6:4	**Cycle Opcode Pointer (COP)** — R/W. This field selects one of the programmed opcodes in the Opcode Menu to be used as the SPI Command/Opcode. In the case of an Atomic Cycle Sequence, this determines the second command.
3	**Sequence Prefix Opcode Pointer (SPOP)** — R/W. This field selects one of the two programmed prefix opcodes for use when performing an Atomic Cycle Sequence. A value of 0 points to the opcode in the least significant byte of the Prefix Opcodes register. By making this programmable, Intel® Xeon® Processor D-1500 Product Family supports flash devices that have different opcodes for enabling writes to the data space versus status register.
2	**Atomic Cycle Sequence (ACS)** — R/W. When set to 1 along with the SCGO assertion, Intel® Xeon® Processor D-1500 Product Family will execute a sequence of commands on the SPI interface without allowing the LAN component to arbitrate and interleave cycles. The sequence is composed of: • Atomic Sequence Prefix Command (8-bit opcode only) • Primary Command specified below by software (can include address and data) • Polling the Flash Status Register (opcode 05h) until bit 0 becomes 0b. The SPI Cycle in Progress bit remains set and the Cycle Done Status bit remains unset until the Busy bit in the Flash Status Register returns 0.
1	**SPI Cycle Go (SCGO)** — R/WS. This bit always returns 0 on reads. However, a write to this register with a '1' in this bit starts the SPI cycle defined by the other bits of this register. The "SPI Cycle in Progress" (SCIP) bit gets set by this action. Hardware must ignore writes to this bit while the Cycle In Progress bit is set. Hardware allows other bits in this register to be programmed for the same transaction when writing this bit to 1. This saves an additional memory write.
0	Reserved



15.4.15 PREOP—Prefix Opcode Configuration Register (GbE LAN Memory Mapped Configuration Registers)

Memory Address: MBARB + 94h Attribute: R/W
Default Value: 0000h Size: 16 bits

Bit	Description
15:8	**Prefix Opcode 1**— R/W. Software programs an SPI opcode into this field that is permitted to run as the first command in an atomic cycle sequence.
7:0	**Prefix Opcode 0** — R/W. Software programs an SPI opcode into this field that is permitted to run as the first command in an atomic cycle sequence.

Note: This register is not writable when the SPI Configuration Lock-Down bit (MBARB + 00h:15) is set.

15.4.16 OPTYPE—Opcode Type Configuration Register (GbE LAN Memory Mapped Configuration Registers)

Memory Address: MBARB + 96h Attribute: R/W
Default Value: 0000h Size: 16 bits

Entries in this register correspond to the entries in the Opcode Menu Configuration register.

Note: The definition below only provides write protection for opcodes that have addresses associated with them. Therefore, any erase or write opcodes that do not use an address should be avoided (for example, "Chip Erase" and "Auto-Address Increment Byte Program").

Bit	Description
15:14	**Opcode Type 7** — R/W. See the description for bits 1:0
13:12	**Opcode Type 6** — R/W. See the description for bits 1:0
11:10	**Opcode Type 5** — R/W. See the description for bits 1:0
9:8	**Opcode Type 4** — R/W. See the description for bits 1:0
7:6	**Opcode Type 3** — R/W. See the description for bits 1:0
5:4	**Opcode Type 2** — R/W. See the description for bits 1:0
3:2	**Opcode Type 1** — R/W. See the description for bits 1:0
1:0	**Opcode Type 0** — R/W. This field specifies information about the corresponding Opcode 0. This information allows the hardware to 1) know whether to use the address field and 2) provide BIOS and Shared Flash protection capabilities. The encoding of the two bits is: 00 = No address associated with this Opcode; Read cycle type 01 = No address associated with this Opcode; Write cycle type 10 = Address required; Read cycle type 11 = Address required; Write cycle type

Note: This register is not writable when the SPI Configuration Lock-Down bit (MBARB + 00h:15) is set.

15.4.17 OPMENU—Opcode Menu Configuration Register (GbE LAN Memory Mapped Configuration Registers)

Memory Address:	MBARB + 98h	Attribute:	R/W
Default Value:	0000000000000000h	Size:	64 bits

Eight entries are available in this register to give GbE a sufficient set of commands for communicating with the flash device, while also restricting what malicious software can do. This keeps the hardware flexible enough to operate with a wide variety of SPI devices.

Note: It is recommended that GbE avoid programming Write Enable opcodes in this menu. Malicious software could then perform writes and erases to the SPI flash without using the atomic cycle mechanism. This could cause functional failures in a shared flash environment. Write Enable opcodes should only be programmed in the Prefix Opcodes.

Bit	Description
63:56	**Allowable Opcode 7** — R/W. See the description for bits 7:0
55:48	**Allowable Opcode 6** — R/W. See the description for bits 7:0
47:40	**Allowable Opcode 5** — R/W. See the description for bits 7:0
39:32	**Allowable Opcode 4** — R/W. See the description for bits 7:0
31:24	**Allowable Opcode 3** — R/W. See the description for bits 7:0
23:16	**Allowable Opcode 2** — R/W. See the description for bits 7:0
15:8	**Allowable Opcode 1** — R/W. See the description for bits 7:0
7:0	**Allowable Opcode 0** — R/W. Software programs an SPI opcode into this field for use when initiating SPI commands through the Control Register.

This register is not writable when the SPI Configuration Lock-Down bit (MBARB + 00h:15) is set.

§

16 Thermal Sensor Registers (D31:F6)

16.1 PCI Bus Configuration Registers

Table 16-1. Thermal Sensor Register Address Map

Offset	Mnemonic	Register Name	Default	Attribute
00h–01h	VID	Vendor Identification	8086h	RO
02h–03h	DID	Device Identification	3A32h	RO
04h–05h	CMD	Command Register	0000h	R/W, RO
06h–07h	STS	Device Status	0010h	R/WC, RO
08h	RID	Revision ID	00h	RO
09h	PI	Programming Interface	00h	RO
0Ah	SCC	Sub Class Code	80h	RO
0Bh	BCC	Base Class Code	11h	RO
0Ch	CLS	Cache Line Size	00h	RO
0Dh	LT	Latency Timer	00h	RO
0Eh	HTYPE	Header Type	00h	RO
10h–13h	TBAR	Thermal Base Address	00000004h	R/W, RO
14h–17h	TBARH	Thermal Base Address High DWord	00000000h	RO
2Ch–2Dh	SVID	Subsystem Vendor Identifier	0000h	R/WO
2Eh–2Fh	SID	Subsystem Identifier	0000h	R/WO
34h	CAP_PTR	Capabilities Pointer	50h	RO
3Ch	INTLN	Interrupt Line	00h	R/W
3Dh	INTPN	Interrupt Pin	See Description	RO
40h–43h	TBARB	BIOS Assigned Thermal Base Address	00000004h	R/W, RO
44h–47h	TBARBH	BIOS Assigned Thermal Base High DWord	00000000h	R/W
50h–51h	PID	PCI Power Management Capability ID	0001h	RO
52h–53h	PC	Power Management Capabilities	0023h	RO
54h–57h	PCS	Power Management Control and Status	0008h	R/W, RO

16.1.1 VID—Vendor Identification Register

Offset Address:	00h–01h	Attribute:	RO
Default Value:	8086h	Size:	16 bit
Lockable:	No	Power Well:	Core

Bit	Description
15:0	**Vendor ID** — RO. This is a 16-bit value assigned to Intel. Intel VID = 8086h

16.1.2 DID—Device Identification Register

Offset Address: 02h–03h
Attribute: RO
Default Value: 3A32h
Size: 16 bits

Bit	Description
15:0	**Device ID (DID)** — RO. Indicates the device number assigned by the SIG.

16.1.3 CMD—Command Register

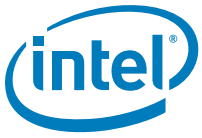
Address Offset: 04h–05h
Attribute: RO, R/W
Default Value: 0000h
Size: 16 bits

Bit	Description
15:11	Reserved
10	**Interrupt Disable (ID)** — R/W. Enables the device to assert an INTx#. 0 = When cleared, the INTx# signal may be asserted. 1 = When set, the Thermal logic's INTx# signal will be de-asserted.
9	FBE (Fast Back to Back Enable) — RO. Hardwired to 0.
8	SEN (SERR Enable) — RO. Hardwired to 0.
7	WCC (Wait Cycle Control) — RO. Hardwired to 0.
6	PER (Parity Error Response) — RO. Hardwired to 0.
5	VPS (VGA Palette Snoop) — RO. Hardwired to 0.
4	MWI (Memory Write and Invalidate Enable) — RO. Hardwired to 0.
3	SCE (Special Cycle Enable) — RO. Hardwired to 0.
2	**BME (Bus Master Enable)** — R/W. 0 = Function disabled as bus master. 1 = Function enabled as bus master.
1	**Memory Space Enable (MSE)** — R/W. 0 = Disable 1 = Enable. Enables memory space accesses to the Thermal registers.
0	IOS (I/O Space) — RO. The Thermal logic does not implement I/O Space; therefore, this bit is hardwired to 0.

16.1.4 STS—Status Register

Address Offset: 06h–07h
Attribute: R/WC, RO
Default Value: 0010h
Size: 16 bits

Bit	Description
15	**Reserved**
14	SERR# Status (SERRS) — RO. Hardwired to 0.
13	Received Master Abort (RMA) — RO. Hardwired to 0.
12	Received Target Abort (RTA) — RO. Hardwired to 0.
11	Signaled Target-Abort (STA) — RO. Hardwired to 0.
10:9	DEVSEL# Timing Status (DEVT) — RO. Hardwired to 0.
8	Master Data Parity Error (MDPE) — RO. Hardwired to 0.
7	Fast Back to Back Capable (FBC) — RO. Hardwired to 0.
6	Reserved
5	66 MHz Capable (C66) — RO. Hardwired to 0.
4	**Capabilities List Exists (CLIST)** — RO. Indicates that the controller contains a capabilities pointer list. The first item is pointed to by looking at configuration offset 34h.
3	**Interrupt Status (IS)** — RO. Reflects the state of the INTx# signal at the input of the enable/disable circuit. This bit is a 1 when the INTx# is asserted. This bit is a 0 after the interrupt is cleared (independent of the state of the Interrupt Disable bit in the command register).



Bit	Description
2:0	Reserved

16.1.5 RID—Revision Identification Register

Address Offset: 08h Attribute: RO
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Revision ID (RID)** — RO. This field indicates the device specific revision identifier.

16.1.6 PI— Programming Interface Register

Address Offset: 09h Attribute: RO
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Programming Interface (PI)** — RO. Intel® Xeon® Processor D-1500 Product Family Thermal logic has no standard programming interface.

16.1.7 SCC—Sub Class Code Register

Address Offset: 0Ah Attribute: RO
Default Value: 80h Size: 8 bits

Bit	Description
7:0	**Sub Class Code (SCC)** — RO. Value assigned to Intel® Xeon® Processor D-1500 Product Family Thermal logic.

16.1.8 BCC—Base Class Code Register

Address Offset: 0Bh Attribute: RO
Default Value: 11h Size: 8 bits

Bit	Description
7:0	**Base Class Code (BCC)** — RO. Value assigned to Intel® Xeon® Processor D-1500 Product Family Thermal logic.

16.1.9 CLS—Cache Line Size Register

Address Offset: 0Ch Attribute: RO
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Cache Line Size (CLS)** — RO. Does not apply to PCI Bus Target-only devices.

16.1.10 LT—Latency Timer Register

Address Offset: 0Dh Attribute: RO
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Latency Timer (LT)** — RO. Does not apply to PCI Bus Target-only devices.

16.1.11 HTYPE—Header Type Register

Address Offset: 0Eh Attribute: RO
Default Value: 00h Size: 8 bits

Bit	Description
7	**Multi-Function Device (MFD)** — RO. This bit is 0 because a multi-function device only needs to be marked as such in Function 0, and the Thermal registers are not in Function 0.
6:0	**Header Type (HTYPE)** — RO. Implements Type 0 Configuration header.

16.1.12 TBAR—Thermal Base Register

Address Offset: 10h–13h Attribute: R/W, RO
Default Value: 00000004h Size: 32 bits

This BAR creates 4K bytes of memory space to signify the base address of Thermal memory mapped configuration registers. This memory space is active when the Command (CMD) register Memory Space Enable (MSE) bit is set and either TBAR[31:12] or TBARH are programmed to a non-zero address. This BAR is owned by the Operating System, and allows the OS to locate the Thermal registers in system memory space.

Bit	Description
31:12	**Thermal Base Address (TBA)** — R/W. This field provides the base address for the Thermal logic memory mapped configuration registers. 4 KB bytes are requested by hardwiring bits 11:4 to 0s.
11:4	Reserved
3	**Prefetchable (PREF)** — RO. Indicates that this BAR is NOT pre-fetchable.
2:1	**Address Range (ADDRNG)** — RO. Indicates that this BAR can be located anywhere in 64 bit address space.
0	**Space Type (SPTYP)** — RO. Indicates that this BAR is located in memory space.

16.1.13 TBARH—Thermal Base High DWord Register

Address Offset: 14h–17h Attribute: R/W, RO
Default Value: 00000000h Size: 32 bits

This BAR extension holds the high 32 bits of the 64 bit TBAR. In conjunction with TBAR, it creates 4 KB of memory space to signify the base address of Thermal memory mapped configuration registers.

Bit	Description
31:0	**Thermal Base Address High (TBAH)** — R/W. TBAR bits 61:32.

16.1.14 SVID—Subsystem Vendor ID Register

Address Offset: 2Ch–2Dh Attribute: R/WO
Default Value: 0000h Size: 16 bits

This register should be implemented for any function that could be instantiated more than once in a given system. The SVID register, in combination with the Subsystem ID register, enables the operating environment to distinguish one subsystem from the other(s).

Software (BIOS) will write the value to this register. After that, the value can be read, but writes to the register will have no effect. The write to this register should be combined with the write to the SID to create one 32-bit write. This register is not affected by $D3_{HOT}$ to D0 reset.

Bit	Description
15:0	**SVID (SVID)** — R/WO. These R/WO bits have no Intel® Xeon® Processor D-1500 Product Family functionality.

16.1.15 SID—Subsystem ID Register

Address Offset: 2Eh–2Fh Attribute: R/WO
Default Value: 0000h Size: 16 bits

This register should be implemented for any function that could be instantiated more than once in a given system. The SID register, in combination with the Subsystem Vendor ID register make it possible for the operating environment to distinguish one subsystem from the other(s).

Software (BIOS) will write the value to this register. After that, the value can be read, but writes to the register will have no effect. The write to this register should be combined with the write to the SVID to create one 32-bit write. This register is not affected by $D3_{HOT}$ to D0 reset.

Bit	Description
15:0	**SID (SAID)** — R/WO. These R/WO bits have no Intel® Xeon® Processor D-1500 Product Family functionality.

16.1.16 CAP_PTR—Capabilities Pointer Register

Address Offset: 34h Attribute: RO
Default Value: 50h Size: 8 bits

Bit	Description
7:0	**Capability Pointer (CP)** — RO. Indicates that the first capability pointer offset is offset 50h (Power Management Capability).

16.1.17 INTLN—Interrupt Line Register

Address Offset: 3Ch Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Interrupt Line** — R/W. Intel® Xeon® Processor D-1500 Product Family hardware does not use this field directly. It is used to communicate to software the interrupt line that the interrupt pin is connected to.

16.1.18 INTPN—Interrupt Pin Register

Address Offset: 3Dh Attribute: RO
Default Value: See description Size: 8 bits

Bit	Description
7:4	Reserved
3:0	**Interrupt Pin** — RO. This reflects the value of the Device 31 interrupt pin bits 27:24 (TTIP) in chipset configuration space.

16.1.19 TBARB—BIOS Assigned Thermal Base Address Register

Address Offset: 40h–43h
Attribute: R/W, RO
Default Value: 00000004h
Size: 32 bits

This BAR creates 4 KB of memory space to signify the base address of Thermal memory mapped configuration registers. This memory space is active when TBARB.SPTYPEN is asserted. This BAR is owned by the BIOS, and allows the BIOS to locate the Thermal registers in system memory space. If both TBAR and TBARB are programmed, then the OS and BIOS each have their own independent "view" of the Thermal registers, and must use the TSIU register to denote Thermal registers ownership/availability.

Bit	Description
31:12	**Thermal Base Address (TBA)** — R/W. This field provides the base address for the Thermal logic memory mapped configuration registers. 4K B bytes are requested by hardwiring bits 11:4 to 0s.
11:4	Reserved
3	**Prefetchable (PREF)** — RO. Indicates that this BAR is NOT pre-fetchable.
2:1	**Address Range (ADDRNG)** — RO. Indicates that this BAR can be located anywhere in 64 bit address space.
0	**Space Type Enable (SPTYPEN)** — R/W. 0 = Disable. 1 = Enable. When set to 1b by software, enables the decode of this memory BAR.

16.1.20 TBARBH—BIOS Assigned Thermal Base High DWord Register

Address Offset: 44h–47h
Attribute: R/W
Default Value: 00000000h
Size: 32 bits

This BAR extension holds the high 32 bits of the 64 bit TBARB.

Bit	Description
31:0	**Thermal Base Address High (TBAH)** — R/W. TBAR bits 61:32.

16.1.21 PID—PCI Power Management Capability ID Register

Address Offset: 50h–51h
Attribute: RO
Default Value: 0001h
Size: 16 bits

Bit	Description
15:8	**Next Capability (NEXT)** — RO. Indicates that this is the last capability structure in the list.
7:0	**Cap ID (CAP)** — RO. Indicates that this pointer is a PCI power management capability

16.1.22 PC—Power Management Capabilities Register

Address Offset: 52h–53h
Attribute: RO
Default Value: 0023h
Size: 16 bits

Bit	Description
15:11	**PME_Support** — RO. Indicates PME# is not supported
10	**D2_Support** — RO. The D2 state is not supported.
9	**D1_Support** — RO. The D1 state is not supported.
8:6	**Aux_Current** — RO. PME# from D3COLD state is not supported, therefore this field is 000b.
5	**Device Specific Initialization (DSI)** — RO. Indicates that device-specific initialization is required.
4	Reserved

Bit	Description
3	PME Clock (PMEC) — RO. Does not apply. Hardwired to 0.
2:0	**Version (VS)** — RO. Indicates support for Revision 1.2 of the *PCI Power Management Specification.*

16.1.23 PCS—Power Management Control And Status Register

Address Offset: 54h–57h Attribute: R/W, RO
Default Value: 0008h Size: 32 bits

Bit	Description
31:24	**Data** — RO. Does not apply. Hardwired to 0s.
23	**Bus Power/Clock Control Enable (BPCCE)** — RO. Hardwired to 0.
22	**B2/B3 Support (B23)** — RO. Does not apply. Hardwired to 0.
21:16	Reserved
15	**PME Status (PMES)** — RO. This bit is always 0, since this PCI Function does not generate PME#.
14:9	**Reserved**
8	**PME Enable (PMEE)** — RO. This bit is always zero, since this PCI Function does not generate PME#.
7:4	Reserved
3	**No Soft Reset** — RO. When set 1, this bit indicates that devices transitioning from $D3_{HOT}$ to D0 because of PowerState commands do not perform an internal reset. Configuration context is preserved. Upon transition from $D3_{HOT}$ to D0 initialized state, no additional operating system intervention is required to preserve Configuration Context beyond writing the PowerState bits.
2	Reserved
1:0	**Power State (PS)** — R/W. This field is used both to determine the current power state of the Thermal controller and to set a new power state. The values are: 00 = D0 state 11 = $D3_{HOT}$ state If software attempts to write a value of 10b or 01b in to this field, the write operation must complete normally; however, the data is discarded and no state change occurs. When in the $D3_{HOT}$ states, the Thermal controller's configuration space is available, but the I/O and memory spaces are not. Additionally, interrupts are blocked. When software changes this value from the $D3_{HOT}$ state to the D0 state, no internal warm (soft) reset is generated.

16.2 Thermal Memory Mapped Configuration Registers (Thermal Sensor – D31:F26)

The base memory for these thermal memory mapped configuration registers is specified in the TBARB (D31:F6:Offset 40h) register. The individual registers are then accessible at TBARB + Offset.

All registers in Table 16-2 are located in the Core Well.

Table 16-2. Thermal Memory Mapped Configuration Register Address Map (Sheet 1 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
00h–01h	TEMP	Temperature	0000h	RO
04h	TSC	Thermal Sensor Control	00h	RO, R/W
06h	TSS	Thermal Sensor Status	00h	RO, R/W, R/WC
08h	TSEL	Thermal Sensor Enable and Lock	00h	RO, R/W
0Ah	TSREL	Thermal Sensor Report Enable and Lock	00h	RO, R/W
0Ch	TSMIC	Thermal Sensor SMI Control	00h	RO, R/W

Table 16-2. Thermal Memory Mapped Configuration Register Address Map (Sheet 2 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
10h–11h	CTT	Catastrophic Trip Point	01FFh	RO, R/W
14h–15h	TAHV	Thermal Alert High Value	0000h	RO, R/W
18h–19h	TALV	Thermal Alert Low Value	0000h	RO, R/W
40h–43h	TL	Throttle Levels	00000000h	RO, R/W
60h–61h	PHL	Intel® Xeon® Processor D-1500 Product Family Hot Level	0000h	RO, R/W
62h	PHLC	PHL Control	00h	RO, R/W
80h	TAS	Thermal Alert Status	00h	RO, R/W, R/WC
82h	TSPIEN	PCI Interrupt Event Enables	00h	RO, R/W
84h	TSGPEN	General Purpose Event Enables	00h	RO, R/W

16.2.1 TEMP—Temperature Register

Offset Address: TBARB+00h Attribute: RO
Default Value: 0000h Size: 16 bit

Bit	Description
15:9	Reserved
8:0	**TS Reading (TSR)** — RO. The die temperature with resolution of 1/2 degree C and an offset of -50C. Thus a reading of 0x121 is 94.5C.

16.2.2 TSC—Thermal Sensor Control Register

Offset Address: TBARB+04h Attribute: RO, R/W
Default Value: 00h Size: 8 bit

This register controls the operation of the thermal sensor.

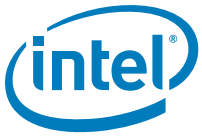
Bit	Description
7	Policy Lock-Down Bit — R/W. When written to 1, this bit prevents any more writes to the register (offset 04h) and to CTT (offset 10h)
6:1	Reserved
0	**Catastrophic Power-Down Enable** — R/W. When set to 1, the power management logic (PMC) transitions to the S5 state when a catastrophic temperature is detected by the sensor. The transition to the S5 state must be unconditional (like the Power Button Override Function). The thermal sensor and response logic is in the core/main power well; therefore, detection of a catastrophic temperature is limited to times when this well is powered and out of reset.

16.2.3 TSS—Thermal Sensor Status Register

Offset Address: TBARB+06h Attribute: RO, R/W
Default Value: 00h Size: 8 bit

This register provides statuses of the thermal sensor.

Bit	Description
7:5	Reserved
4	**Thermal Sensor Dynamic Shutdown Status (TSDSS)** — RO. This bit indicates the status of the thermal sensor circuit when TSEL.ETS=1. 1 = thermal sensor is fully operational 0 = thermal sensor is in a dynamic shutdown state



Bit	Description
3	**GPE Status (GPES)** — R/WC. Set when GPE is enabled for a trip event. Software must write a '1' to this bit to clear the GPE status. GPE can be configured to cause an SMI or SCI. As long as this bit is set, the GPE indication to the global GPE logic is asserted.
2	**SMI Status (SMIS)** — R/WC. Set when SMI is enabled for a trip event. Software must write a '1' to this bit to clear the SMI status. As long as this bit is set, the SMI indication to the global SMI logic is asserted.
1:0	Reserved

16.2.4 TSEL — Thermal Sensor Enable and Lock Register

Offset Address: TBARB+08h Attribute: RO, R/W
Default Value: 00h Size: 8 bit

This register controls the operation of the thermal sensor.

Bit	Description
7	**Policy Lock-Down Bit** — R/W. When written to 1, this bit prevents any more writes to this register.
6:1	Reserved
0	Enable TS (ETS) — R/W. 1 = Enables the thermal sensor. Until this bit is set, no thermometer readings or trip events will occur. If SW reads the TEMP register before the sensor is enabled, it will read 0x0. The value of this bit is sent to the thermal sensor. **NOTE**: if the sensor is running and valid temperatures have been captured in TEMP and then ETS is cleared, TEMP will retain its old value. Clearing ETS does not force TEMP to 0x00. 0 = Disables the sensor.

16.2.5 TSREL—Thermal Sensor Reporting Enable and Lock Register

Offset Address: TBARB+0Ah Attribute: RO, R/W
Default Value: 00h Size: 8 bit

Bit	Description
7	**Policy Lock-Down Bit** — R/W. When written to 1, this bit prevents anymore writes to this register.
6:1	Reserved
0	**Enable SMBus Temperature Reporting**— R/W. 1 = Enables the reporting of Intel® Xeon® Processor D-1500 Product Family temperature to the SMBus and PMC. This must also be set if ME needs access to Intel® Xeon® Processor D-1500 Product Family temperature. Once enabled this bit should not be cleared by software. If it is cleared then the EC may get an undefined value. Software has no need to dynamically disable and then re-enable this bit. 0 = Disables temperature reporting.

16.2.6 TSMIC—Thermal Sensor SMI Control Register

Offset Address: TBARB+0Ch Attribute: RO, R/W
Default Value: 00h Size: 8 bit

Bit	Description
7	**Policy Lock-Down Bit** — R/W. When written to 1, this bit prevents anymore writes to this register.
6:1	Reserved
0	**SMI Enable on Alert Thermal Sensor Trip** — R/W. 1 = Enables SMI# assertions on alert thermal sensor events for either low-to-high or high-to-low events. Both edges are enabled by this one bit. 0 = Disables SMI# assertions for alert thermal events.

16.2.7 CTT—Catastrophic Trip Point Register

Offset Address: TBARB+10h
Attribute: RO, R/W
Default Value: 01FFh
Size: 16 bit

Bit	Description
15:9	Reserved
8:0	**Catastrophic Temperature TRIP (CTRIP)** — R/W. When the current temperature reading is greater than or equal to the value in this register, a catastrophic trip event is signaled. This register is locked by TSC[7]

16.2.8 TAHV—Thermal Alert High Value Register

Offset Address: TBARB+14h
Attribute: RO, R/W
Default Value: 0000h
Size: 16 bit

Bit	Description
15:9	Reserved
8:0	**Alert High (AH)** — R/W. Sets the high value for the alert indication. See the later section for usage. ***Note:*** It is illegal for SW to program AH to a value less than TALV.AL. This register is not lockable, so that SW can change the values during runtime.

16.2.9 TALV—Thermal Alert Low Value Register

Offset Address: TBARB+18h
Attribute: R/W, RO
Default Value: 0000h
Size: 16 bit

Bit	Description
15:9	Reserved
8:0	**Alert Low (AL)** — R/W. Sets the low value for the alert indication. See the later section for usage. This register is not lockable, so that SW can change the values during runtime.

16.2.10 TL—Throttle Levels Register

Offset Address: TBARB+40h
Attribute: RO, R/W
Default Value: 00000000h
Size: 32 bit

Bit	Description
31	**TT.Lock** – R/W. When set to '1', this entire register (TL) is locked and remains locked until the next platform reset.
30	**TT.State13 Enable (TT13EN)** – R/W. When set to '1' and the programmed GPIO pin is a '1', then PMSync state 13 will force at least T2 state.
29	**TT Enable (TTEN) –** R/W. When set the thermal throttling states are enabled. At reset, BIOS must set bits 28:0 and then do a separate write to set bit 29 to enable throttling. SW may set bit 31 at the same time it sets bit 29 if it wishes to lock the register. If SW wishes to change the values of 28:0, it must first clear the TTEN bit, then change the values in 28:0; and then re-enable TTEN. It is legal to set bits 31, 30 and 29 with the same write. This bit must not be set by SW until SW has already enabled the thermal sensor(TSEL.ETS ='1'). If TTEN is written to '0', after having been enabled, then Intel® Xeon® Processor D-1500 Product Family may stay in the throttling state it was in at the moment TTEN is disabled. There is no intent that the sensor be enabled for a while and then disabled and left off. It may be disabled temporarily while changing the register values, but it should not be left in the disabled state.

Bit	Description
28:20	**T2 Level (T2L) –** R/W. When TTEN = 1 AND TSE = '1' AND (T2L >= TSR[8:0] > T1L), then the system is in T2 state. When TTEN = 1 AND TSE = '1' AND (TSR[8:0] > T2L), then the system is in T3 state. ***Note:*** The T3 condition overrides PMSync[13] and forces the system to T3 if both cases are true. **SW NOTE:**T2L must be programmed to a value greater than T1L if TTEN='1'
19	Reserved
18:10	**T1 Level (T1L) –** R/W. When TTEN = 1 AND TSE = 1 AND (T1L >= TSR[8:0] > T0L), then the system is in T1 state. **SW NOTE**:T1L must be programmed to a value greater than T0L if TTEN='1'
9	Reserved
8:0	**T0 Level (T0L)** – R/W. When TEMP.TSR[8:0] <= T0L OR TT.Enable is '0' OR TSE 0', then the system is in T0 state.

16.2.11 PHL—Intel® Xeon® Processor D-1500 Product Family Hot Level Register

Offset Address: TBARB+60h Attribute: RO, R/W
Default Value: 0000h Size: 16 bit

Bit	Description
15	**PHL Enable (PHLE)** – R/W. When set and the current temperature reading, TSR, is greater than PHLL, then the TEMP_ALERT# pin will be asserted (active low).
14:9	Reserved
8:0	**PHL Level (PHLL)** – R/W. Temperature value used for TEMP_ALERT# pin.

16.2.12 PHLC—PHL Control Register

Offset Address: TBARB+62h Attribute: RO, R/W
Default Value: 00h Size: 8 bit

Bit	Description
7:1	Reserved
0	**PHL Lock** – R/W. When written to a '1', then both PHL and PHLC are locked

16.2.13 TAS — Thermal Alert Status Register

Offset Address: TBARB+80h Attribute: RO, R/W
Default Value: 00h Size: 8 bit

Bit	Description
7:2	Reserved
1	**Alert High-to-Low Event (AHLE)** — R/WC. 1 = Indicates that a Hot Thermal Sensor trip event occurred based on a lower to higher temperature transition thru the trip point. 0 = No trip for this event Software must write a 1 to clear this status bit.

Bit	Description
0	**Alert Low-to-High Event (ALHE)** — R/WC. 1 = Indicates that an Aux Thermal Sensor trip event occurred based on a lower to higher temperature transition thru the trip point. 0 = No trip for this event Software must write a 1 to clear this status bit. ***Note:*** AHLE will not be set until there has been one occurrence of a Low to High event (ALHE must have been set once). This prevents the case where the system power up at a reasonably high temperature and starts to cool off while booting and causing an interrupt before there is SW loaded to handle it.

16.2.14 TSPIEN — PCI Interrupt Event Enables Register

Offset Address: TBARB+82h Attribute: RO, R/W
Default Value: 00h Size: 8 bit

Bit	Description
7:2	Reserved
1	**Alert High-to-Low Enable** — R/W. When set to 1, the thermal sensor logic asserts the Thermal logic PCI INTx signal when the corresponding status bit is set in the Thermal Error Status register. When cleared, the corresponding status bit does not result in PCI INTx.
0	**Alert Low-to-High Enable** — R/W. See the description for bit 1

16.2.15 TSGPEN—General Purpose Event Enables Register

Offset Address: TBARB+84h Attribute: RO, R/W
Default Value: 00h Size: 8 bit

Bit	Description
7:2	Reserved
1	**Alert High-to-Low Enable** — R/W. When set to 1, the thermal sensor logic asserts its General Purpose Event signal to the GPE block when the corresponding status bit is set in the Thermal Error Status register. When cleared, the corresponding status bit does not result in the GPE signal assertion.
	Alert Low-to-High Enable — R/W. See the description for bit 1.

§

17 Intel® Management Engine Subsystem Registers (D22:F[3:0])

17.1 First Intel® Management Engine Interface (Intel® MEI) Configuration Registers (Intel® MEI 1 — D22:F0)

17.1.1 PCI Configuration Registers (Intel® MEI 1—D22:F0)

Table 17-1. Intel® MEI 1 Configuration Registers Address Map (Intel® MEI 1—D22:F0) (Sheet 1 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
00h–01h	VID	Vendor Identification	8086h	RO
02h–03h	DID	Device Identification	See register description	RO
04h–05h	PCICMD	PCI Command	0000h	R/W, RO
06h–07h	PCISTS	PCI Status	0010h	RO
08h	RID	Revision Identification	See register description	RO
09h–0Bh	CC	Class Code	078000h	RO
0Eh	HTYPE	Header Type	80h	RO
10h–17h	MEI0_MBAR	Intel MEI 1 MMIO Base Address	0000000000000004h	R/W, RO
2Ch–2Dh	SVID	Subsystem Vendor ID	0000h	R/WO
2Eh–2Fh	SID	Subsystem ID	0000h	R/WO
34h	CAPP	Capabilities List Pointer	50h	RO
3Ch–3Dh	INTR	Interrupt Information	0100h	R/W, RO
40h–43h	HFS	Host Firmware Status	00000000h	RO
44h–47h	ME_UMA	Intel® ME UMA Register	10000000h	RO
48h–4Bh	GMES	General Intel® ME Status	00000000h	RO
4Ch–4Fh	H_GS	Host General Status	00000000h	R/W
50h–51h	PID	PCI Power Management Capability ID	8C01h	RO
52h–53h	PC	PCI Power Management Capabilities	C803h	RO
54h–55h	PMCS	PCI Power Management Control and Status	0008h	R/WC, R/W, RO
60h-63h	GMES2	General Intel® ME Status 2	00000000h	RO
64h-67h	GMES3	General Intel® ME Status 3	00000000h	RO
68h-6Bh	GMES4	General Intel® ME Status 4	00000000h	RO
6Ch-6Fh	GMES5	General Intel® ME Status 5	00000000h	RO
70h-73h	H_GS2	Host General Status 2	00000000h	RW
74h-77h	H_GS3	Host General Status 3	00000000h	RW

Table 17-1. Intel® MEI 1 Configuration Registers Address Map (Intel® MEI 1—D22:F0) (Sheet 2 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
8Ch–8Dh	MID	Message Signaled Interrupt Identifiers	0005h	RO
8Eh–8Fh	MC	Message Signaled Interrupt Message Control	0080h	R/W, RO
90h–93h	MA	Message Signaled Interrupt Message Address	00000000h	R/W, RO
94h–97h	MUA	Message Signaled Interrupt Upper Address	00000000h	R/W
98h–99h	MD	Message Signaled Interrupt Message Data	0000h	R/W
A0h	HIDM	Intel MEI Interrupt Delivery Mode	00h	R/W
BCh–BFh	HERES	Intel MEI Extended Register Status	40000000h	RO
C0h–DFh	HER[1:8]	Intel MEI Extended Register DW[1:8]	00000000h	RO

17.1.1.1 VID—Vendor Identification Register (Intel® MEI 1—D22:F0)

Address Offset: 00h–01h
Attribute: RO
Default Value: 8086h
Size: 16 bits

Bit	Description
15:0	**Vendor ID (VID)** — RO. This is a 16-bit value assigned to Intel.

17.1.1.2 DID—Device Identification Register (Intel® MEI 1—D22:F0)

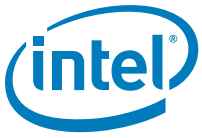
Address Offset: 02h–03h
Attribute: RO
Default Value: See bit description
Size: 16 bits

Bit	Description
15:0	**Device ID (DID)** — RO. This is a 16-bit value assigned to the Intel® ME Interface controller. See the *Specification Update* for the value of the DID Register.

17.1.1.3 PCICMD—PCI Command Register (Intel® MEI 1—D22:F0)

Address Offset: 04h–05h
Attribute: R/W, RO
Default Value: 0000h
Size: 16 bits

Bit	Description
15:11	Reserved
10	**Interrupt Disable (ID)** — R/W. Disables this device from generating PCI line based interrupts. This bit does not have any effect on MSI operation.
9:3	Reserved
2	Bus Master Enable (BME)— R/W. Controls the Intel® MEI host controller's ability to act as a system memory master for data transfers. When this bit is cleared, Intel® ME bus master activity stops and any active DMA engines return to an idle condition. This bit is made visible to firmware through the H_PCI_CSR register, and changes to this bit may be configured by the H_PCI_CSR register to generate an Intel® ME MSI. When this bit is 0, Intel® MEI is blocked from generating MSI to the host processor. ***Note:*** This bit does not block Intel® MEI accesses to Intel® ME UMA; that is, writes or reads to the host and Intel® ME circular buffers through the read window and write window registers still cause Intel® ME backbone transactions to Intel® ME UMA.
1	**Memory Space Enable (MSE)** — R/W. Controls access to the Intel® ME's memory mapped register space. 0 = Disable. Memory cycles within the range specified by the memory base and limit registers are master aborted. 1 = Enable. Allows memory cycles within the range specified by the memory base and limit registers accepted.
0	Reserved



17.1.1.4 PCISTS—PCI Status Register (Intel® MEI 1—D22:F0)

Address Offset:	06h–07h	Attribute:	RO
Default Value:	0010h	Size:	16 bits

Bit	Description
15:5	**Reserved**
4	Capabilities List (CL) — RO. Indicates the presence of a capabilities list, hardwired to 1.
3	**Interrupt Status (IS)** — RO. Indicates the interrupt status of the device. 0 = Interrupt is deasserted. 1 = Interrupt is asserted.
2:0	Reserved

17.1.1.5 RID—Revision Identification Register (Intel® MEI 1—D22:F0)

Offset Address:	08h	Attribute:	RO
Default Value:	See bit description	Size:	8 bits

Bit	Description
7:0	**Revision ID** — RO. See the *Specification Update* for the value of the RID Register.

17.1.1.6 CC—Class Code Register (Intel® MEI 1—D22:F0)

Address Offset:	09h–0Bh	Attribute:	RO
Default Value:	078000h	Size:	24 bits

Bit	Description
23:16	**Base Class Code (BCC)** — RO. Indicates the base class code of the Intel MEI device.
15:8	**Sub Class Code (SCC)** — RO. Indicates the sub class code of the Intel MEI device.
7:0	**Programming Interface (PI)** — RO. Indicates the programming interface of the Intel MEI device.

17.1.1.7 HTYPE—Header Type Register (Intel® MEI 1—D22:F0)

Address Offset:	0Eh	Attribute:	RO
Default Value:	80h	Size:	8 bits

Bit	Description
7	**Multi-Function Device (MFD)** — RO. Indicates the Intel® MEI host controller is part of a multifunction device.
6:0	**Header Layout (HL)** — RO. Indicates that the Intel® MEI uses a target device layout.

17.1.1.8 MEI0_MBAR—Intel MEI 1 MMIO Base Address (Intel® MEI 1—D22:F0)

Address Offset:	10h–17h	Attribute:	R/W, RO
Default Value:	0000000000000004h	Size:	64 bits

This register allocates space for the MEI0 memory mapped registers.

Bit	Description
63:4	**Base Address (BA)** — R/W. Software programs this field with the base address of this region.
3	**Prefetchable Memory (PM)** — RO. Indicates that this range is not pre-fetchable.
2:1	**Type (TP)** — RO. Set to 10b to indicate that this range can be mapped anywhere in 64-bit address space.
0	**Resource Type Indicator (RTE)** — RO. Indicates a request for register memory space.

17.1.1.9 SVID—Subsystem Vendor ID Register (Intel® MEI 1—D22:F0)

Address Offset: 2Ch–2Dh Attribute: R/WO
Default Value: 0000h Size: 16 bits

Bit	Description
15:0	**Subsystem Vendor ID (SSVID)** — R/WO. Indicates the sub-system vendor identifier. This field should be programmed by BIOS during boot-up. Once written, this register becomes Read Only. This field can only be cleared by PLTRST#. ***Note:*** Register must be written as a Word write or as a DWord write with SID register.

17.1.1.10 SID—Subsystem ID Register (Intel® MEI 1—D22:F0)

Address Offset: 2Eh–2Fh Attribute: R/WO
Default Value: 0000h Size: 16 bits

Bit	Description
15:0	**Subsystem ID (SSID)** — R/WO. Indicates the sub-system identifier. This field should be programmed by BIOS during boot-up. Once written, this register becomes Read Only. This field can only be cleared by PLTRST#. ***Note:*** Register must be written as a Word write or as a DWord write with SVID register.

17.1.1.11 CAPP—Capabilities List Pointer Register (Intel® MEI 1—D22:F0)

Address Offset: 34h Attribute: RO
Default Value: 50h Size: 8 bits

Bit	Description
7:0	**Capabilities Pointer (PTR)** — RO. Indicates that the pointer for the first entry in the capabilities list is at 50h in configuration space.

17.1.1.12 INTR—Interrupt Information Register (Intel® MEI 1—D22:F0)

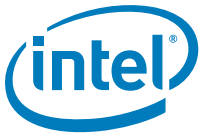
Address Offset: 3Ch–3Dh Attribute: R/W, RO
Default Value: 0100h Size: 16 bits

Bit	Description
15:8	**Interrupt Pin (IPIN)** — RO. This indicates the interrupt pin the Intel® MEI host controller uses. A value of 1h/2h/3h/4h indicates that this function implements legacy interrupt on INTA/INTB/INTC/INTD, respectively.
7:0	**Interrupt Line (ILINE)** — R/W. Software written value to indicate which interrupt line (vector) the interrupt is connected to. No hardware action is taken on this register.

17.1.1.13 HFS— Intel® ME Host Firmware Status Register (Intel® MEI 1—D22:F0)

Address Offset: 40h–43h Attribute: RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:28	**BIOS MSG ACK**: Acknowledge for register based BIOS message in MEI 1 H_GS Register.
27:25	**BIOS MSG ACK Data**: Message specific data for acknowledged BIOS message.
24:20	Reserved
19:16	**Operating Mode:** This field describes the current operating mode of Intel® ME. 1:0 – Reserved 2 – Debug Mode 14:3 – Reserved 15 – Intel® SPS firmware is running in Intel® ME



Bit	Description
15:12	**Error Code:** If set to nonzero value the Intel® ME firmware has encountered a fatal error and stopped normal operation. 0 – No Error 1 – Uncategorized Failure – The Intel® ME firmware has experienced an uncategorized error. Further details of the failure can be found in the Extended Status Data. 2 – Disabled – Firmware was disabled on this platform. 3 – Image Failure - The Intel® ME firmware stored in the system flash is not valid.
11	**Update in Progress:** This bit is set if any type of Intel® ME firmware update is in progress.
10	**Recovery BUP Load Fault**: This bit is set when firmware is not able to load recovery bring-up from the flash. It means that the recovery section in Intel® ME region is broken. When this bit set, it may or may not have the error code shown in bit [15:12]. The reason is because the firmware can load bring-up from the operational code. The system can get this bit clear only by update of the recovery section in Intel® ME region, or re-flashing the whole Intel® ME region on the SPI flash.
9	**Init Complete**: When this bit is not set firmware is still in initialization phase. When firmware has fully entered a stable state, this bit is set to 1 and "Current State" field of this register provides the steady state of the Intel® ME subsystem.
8:6	**Operating State**: This field describes the current operating state of Intel® ME. 000 – Preboot 001 – M0 with UMA 010 – Reserved 011 – Reserved 100 – M3 without UMA 101 – M0 without UMA – normal state for Intel® SPS firmware 110 – Bring up 111 – M0 without UMA but with error
5	**FPT or Factory Defaults Bad**: This bit is set when the firmware discovers a bad checksum of Intel® ME region Flash Partition Table (FPT) or Factory Defaults. When this bit set, it may or may not have the error code shown in bit [15:12]. The system can get this bit clear only by re-flashing the whole Intel® ME region in the SPI flash.
4	**Manufacturing Mode**: When this bit is set, the platform is still in manufacturing mode. Host can use this bit to inform user that the platform is NOT READY for production yet. This bit is set as long as Intel® ME Region access is not locked for flash masters other than Intel® ME. For shipping machine, this bit MUST be 0.
3:0	**Current State:** This field describes the current operation state of the firmware. 0 – Reset – Intel® ME is in reset state, will exit this state within 1 millisecond 1 – Initialization – Intel® ME is initializing, will exit this state within 2 seconds 2 – Recovery – Intel® ME is in recovery mode, check ME1.GMES register to determine cause 3 – Reserved 4 – Disabled – Intel® ME functionality has been disabled, it executes idle loop 5 – Operational – Intel® ME is in normal operational state 6 – Reserved 7 – State Transition – Intel® ME sets this state before starting a transition to a new Operating State. It is temporary state, may appear on transition between Initialization and Operational.

17.1.1.14 ME_UMA—Intel® Management Engine UMA Register (Intel® MEI 1—D22:F0)

Address Offset: 44h–47h
Default Value: 80000000h
Attribute: RO
Size: 32 bits

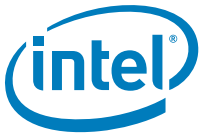
Bit	Description
31	Reserved — RO. Hardwired to 1. Can be used by host software to discover that this register is valid.
30:7	Reserved
16	**Intel® ME UMA Size Valid**—RO. This bit indicates that FW has written to the MUSZ field.
15:6	Reserved

Bit	Description
5:0	**Intel® ME UMA Size (MUSZ)—**RO. This field reflect Intel® Server Platform Services' FW desired size of Intel® ME UMA memory region. This field is set by Intel® Server Platform Services FW prior to core power bring up allowing BIOS to initialize memory. 000000b = 0 MB, No memory allocated to Intel ME UMA 000001b = 1 MB 000010b = 2 MB 000100b = 4 MB 001000b = 8 MB 010000b = 16 MB 100000b = 32 MB

17.1.1.15 GMES—General Intel® ME Status Register (Intel® MEI 1—D22:F0)

Address Offset: 48h–4Bh
Attribute: RO
Default Value: 00000000h
Size: 32 bits

Bit	Description
31	**EOP Status:** This bit presents the Intel® ME notion of EOP status. If BIOS encounters this bit set to '1' during POST it signals an error in platform power flow.
30:28	**Infrastructure Progress Code:** This field identifies the infrastructure progress code. 0 – ROM – Intel® ME is in ROM phase 1 – BUP – Intel® ME is in BRINGUP phase 2 – uKernel –Intel® ME is in Micro Kernel phase 3 – Policy Module – Intel® ME is in Policy Module phase 4 – Other Module – Intel® ME is loading modules in MO or M3 Operating State
27:16	**Extended Status Data**: These bits provide extended status data for the current state of operation of the firmware. Or, if the firmware is in a fatal error state, these bits provide extended error code information.
15:13	**Firmware Heartbeat:** This number increments approximately every second if Intel® ME firmware is running.
12	Intel® ME Target Image Boot Fault 0 – target image loaded successfully 1 – target image boot failed, switched to backup image or recovery image
11:8	Reserved
7	**Warm Reset Request:** If this bit is set, Intel® ME informs BIOS that a warm reset is requested by Intel® ME.
6	**MFS Failure:** If this bit is set Intel® ME informs the BIOS that Intel® ME File System failure has been detected during recent Intel® ME boot.
5:4	Reserved
3:1	**Recovery Cause:** If ME1.HFS.Current State indicates that Intel® ME firmware is running in recovery mode these bits provide the cause of this mode: 0 – Intel® ME recovery jumper asserted 1 – Security strap override jumper asserted 2 – Recovery forced with IPMI command 3 – Invalid flash configuration, either: - flash master access permissions configuration is wrong - VSCC entry is missing or wrong - flash erase block size in Intel® ME region configuration 4 – Intel® ME internal error Intel® ME could not start in operational mode because of some firmware problems. 5..7 – reserved for future extensions
0	**BIST in Progress:** If this bit is set Intel® ME Built In Self-Test is in progress.



17.1.1.16 H_GS—Host General Status Register (Intel® MEI 1—D22:F0)

Address Offset:	4Ch–4Fh	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits

Bit	Description
31:28	**Command**: Command code.
27:0	**Data: C**ommand specific data.

17.1.1.17 PID—PCI Power Management Capability ID Register (Intel® MEI 1—D22:F0)

Address Offset:	50h–51h	Attribute:	RO
Default Value:	8C01h	Size:	16 bits

Bit	Description
15:8	**Next Capability (NEXT)** — RO. Value of 8Ch indicates the location of the next pointer.
7:0	**Capability ID (CID)** — RO. Indicates the linked list item is a PCI Power Management Register.

17.1.1.18 PC—PCI Power Management Capabilities Register (Intel® MEI 1—D22:F0)

Address Offset:	52h–53h	Attribute:	RO
Default Value:	C803h	Size:	16 bits

Bit	Description
15:11	**PME_Support (PSUP)** — RO. This five-bit field indicates the power states in which the function may assert PME#. Intel® MEI can assert PME# from any D-state except D1 or D2 which are not supported by Intel® MEI.
10:9	Reserved
8:6	**Aux_Current (AC)** — RO. Reports the maximum Suspend well current required when in the $D3_{cold}$ state. Value of 00b is reported.
5	**Device Specific Initialization (DSI)** — RO. Indicates whether device-specific initialization is required.
4	Reserved
3	**PME Clock (PMEC)** — RO. Indicates that PCI clock is not required to generate PME#.
2:0	**Version (VS)** — RO. Hardwired to 011b to indicate support for *Revision 1.2 of the PCI Power Management Specification*.

17.1.1.19 PMCS—PCI Power Management Control and Status Register (Intel® MEI 1—D22:F0)

Address Offset:	54h–55h	Attribute:	R/WC, R/W, RO
Default Value:	0008h	Size:	16 bits

Bit	Description
15	**PME Status (PMES)** — R/WC. Bit is set by Intel® Server Platform Services Firmware. Host software clears bit by writing '1' to bit. This bit is reset when CL_RST# asserted.
14:9	Reserved
8	**PME Enable (PMEE)** — R/W. This bit is read/write and is under the control of host SW. It does not directly have an effect on PME events. However, this bit is shadowed so Intel® Server Platform Services FW can monitor it. Intel® Server Platform Services FW will not cause the PMES bit to transition to 1 while the PMEE bit is 0, indicating that host SW had disabled PME. This bit is reset when PLTRST# asserted.
7:4	Reserved
3	**No_Soft_Reset (NSR)** — RO. This bit indicates that when the Intel® MEI host controller is transitioning from $D3_{hot}$ to D0 due to a power state command, it does not perform an internal reset. Configuration context is preserved.

Bit	Description
2	Reserved
1:0	**Power State (PS)** — R/W. This field is used both to determine the current power state of the Intel® MEI host controller and to set a new power state. The values are: 00 = D0 state (default) 11 = $D3_{hot}$ state The D1 and D2 states are not supported for the Intel® MEI host controller. When in the $D3_{hot}$ state, the Intel® ME's configuration space is available, but the register memory spaces are not. Additionally, interrupts are blocked.

17.1.1.20 GMES2—General Intel® ME Status Register 2 (Intel® MEI 1—D22:F0)

Address Offset: 60h–63h Attribute: RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:0	**General Intel® ME Status 2(ME_GS 2)**— RO. This field is populated by Intel® ME.

17.1.1.21 GMES3—General Intel® ME Status Register 3 (Intel® MEI 1—D22:F0)

Address Offset: 64h–67h Attribute: RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:0	**General Intel® ME Status 3 (ME_GS 3)**— RO. This field is populated by Intel® ME.

17.1.1.22 GMES4—General Intel® ME Status Register 4 (Intel® MEI 1—D22:F0)

Address Offset: 68h–6Bh Attribute: RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:0	**General Intel® ME Status 4 (ME_GS 4)**— RO. This field is populated by Intel® ME.

17.1.1.23 GMES5—General Intel® ME Status Register 5 (Intel® MEI 1—D22:F0)

Address Offset: 6Ch–6Fh Attribute: RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:0	**General Intel® ME Status 5 (ME_GS 5)**— RO. This field is populated by Intel® ME.

17.1.1.24 H_GS2—Host General Status Register 2 (Intel® MEI 1—D22:F0)

Address Offset: 70h–73h Attribute: R/W
Default Value: 00000000h Size: 32 bits

Bit	Description
31:0	**Host General Status 2 (H_GS 2)**— R/W. General Status of Host, this field is not used by Hardware

17.1.1.25 H_GS3—Host General Status Register 3 (Intel® MEI 1—D22:F0)

Address Offset: 74h–77h Attribute: R/W
Default Value: 00000000h Size: 32 bits

Bit	Description
31:0	**Host General Status 3 (H_GS3)**— R/W. General Status of Host, this field is not used by Hardware

17.1.1.26 MID—Message Signaled Interrupt Identifiers Register (Intel® MEI 1—D22:F0)

Address Offset: 8Ch-8Dh
Default Value: 0005h
Attribute: RO
Size: 16 bits

Bit	Description
15:8	**Next Pointer (NEXT)** — RO. Value of 00h indicates that this is the last item in the list.
7:0	**Capability ID (CID)** — RO. Capabilities ID indicates MSI.

17.1.1.27 MC—Message Signaled Interrupt Message Control Register (Intel® MEI 1—D22:F0)

Address Offset: 8Eh–8Fh
Default Value: 0080h
Attribute: R/W, RO
Size: 16 bits

Bit	Description
15:8	Reserved
7	**64 Bit Address Capable (C64)** — RO. Specifies that function is capable of generating 64-bit messages.
6:1	Reserved
0	**MSI Enable (MSIE)** — R/W. If set, MSI is enabled and traditional interrupt pins are not used to generate interrupts.

17.1.1.28 MA—Message Signaled Interrupt Message Address Register (Intel® MEI 1—D22:F0)

Address Offset: 90h–93h
Default Value: 00000000h
Attribute: R/W, RO
Size: 32 bits

Bit	Description
31:2	**Address (ADDR)** — R/W. Lower 32 bits of the system specified message address, always DW aligned.
1:0	Reserved

17.1.1.29 MUA—Message Signaled Interrupt Upper Address Register (Intel® MEI 1—D22:F0)

Address Offset: 94h–97h
Default Value: 00000000h
Attribute: R/W
Size: 32 bits

Bit	Description
31:0	**Upper Address (UADDR)** — R/W. Upper 32 bits of the system specified message address, always DW aligned.

17.1.1.30 MD—Message Signaled Interrupt Message Data Register (Intel® MEI 1—D22:F0)

Address Offset: 98h–99h
Default Value: 0000h
Attribute: R/W
Size: 16 bits

Bit	Description
15:0	**Data (DATA)** — R/W. This 16-bit field is programmed by system software if MSI is enabled. Its content is driven during the data phase of the MSI memory write transaction.

17.1.1.31 HIDM—MEI Interrupt Delivery Mode Register (Intel® MEI 1—D22:F0)

Address Offset:	A0h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

Bit	Description
7:2	Reserved
1:0	**Intel® MEI Interrupt Delivery Mode (HIDM)** — R/W. These bits control what type of interrupt the Intel® MEI will send the host. They are interpreted as follows: 00 = Generate Legacy or MSI interrupt 01 = Generate SCI 10 = Generate SMI

17.1.1.32 HERES—Intel® MEI Extend Register Status (Intel® MEI 1—D22:F0)

Address Offset:	BCh–BFh	Attribute:	RO
Default Value:	40000000h	Size:	32 bits

Bit	Description
31	**Extend Register Valid (ERV)** - RO. Set by firmware after all firmware has been loaded. If ERA field is SHA-1, the result of the extend operation is in HER:5-1. If ERA field is SHA-256, the result of the extend operation is in HER:8-1.
30	**Extend Feature Present (EFP)** - RO. This bit is hardwired to 1 to allow driver software to easily detect the chipset supports the Extend Register FW measurement feature.
29:4	Reserved
3:0	**Extend Register Algorithm (ERA)** - RO. This field indicates the hash algorithm used in the FW measurement extend operations. Encodings are: 0h = SHA-1 2h = SHA-256 Other values = Reserved.

17.1.1.33 HERX—Intel® MEI Extend Register DWX (Intel® MEI 1—D22:F0)

Address Offset:	HER1: C0h–C3h HER2: C4h–C7h HER3: C8h–CBh HER4: CCh–CFh HER5: D0h–D3h HER6: D4h–D7h HER7: D8h–DBh HER8: DCh–DFh	Attribute:	RO
Default Value:	00000000h	Size:	32 bits

Bit	Description
31:0	**Extend Register DWX (ERDWX) - RO.** Xth DWORD result of the extend operation. ***Note:*** Extend Operation is HER[5:1] if using SHA-1. If using SHA-256 then Extend Operation is HER[8:1]

17.1.2 MEI0_MBAR—Intel® MEI 1 MMIO Registers

These MMIO registers are accessible starting at the Intel® MEI 1 MMIO Base Address (MEI0_MBAR) which gets programmed into D22:F0:Offset 10–17h. These registers are reset by PLTRST# unless otherwise noted.

Table 17-2. Intel® MEI 1 MMIO Register Address Map

MEI0_MBAR+Offset	Mnemonic	Register Name	Default	Attribute
00–03h	H_CB_WW	Host Circular Buffer Write Window	00000000h	W
04h–07h	H_CSR	Host Control Status	02000000h	RO, R/W, R/WC
08h–0Bh	ME_CB_RW	Intel® ME Circular Buffer Read Window	FFFFFFFFh	RO
0Ch–0Fh	ME_CSR_HA	Intel® ME Control Status Host Access	02000000h	RO

17.1.2.1 H_CB_WW—Host Circular Buffer Write Window Register (Intel® MEI 1 MMIO Register)

Address Offset: MEI0_MBAR + 00h
Attribute: W
Default Value: 00000000h
Size: 32 bits

Bit	Description
31:0	**Host Circular Buffer Write Window Field (H_CB_WWF)**. This bit field is for host to write into its circular buffer. The host's circular buffer is located at the Intel® ME subsystem address specified in the Host CB Base Address register. This field is write only, reads will return arbitrary data. Writes to this register will increment the H_CBWP as long as ME_RDY is 1. When ME_RDY is 0, writes to this register have no effect and are not delivered to the H_CB, nor is H_CBWP incriminated.

17.1.2.2 H_CSR—Host Control Status Register (Intel® MEI 1 MMIO Register)

Address Offset: MEI0_MBAR + 04h
Attribute: RO, R/W, R/WC
Default Value: 02000000h
Size: 32 bits

Bit	Description
31:24	**Host Circular Buffer Depth (H_CBD)** — RO. This field indicates the maximum number of 32 bit entries available in the host circular buffer (H_CB). Host software uses this field along with the H_CBRP and H_CBWP fields to calculate the number of valid entries in the H_CB to read or # of entries available for write. This field is implemented with a "1-hot" scheme. Only one bit will be set to a "1" at a time. Each bit position represents the value n of a buffer depth of (2^n). For example, when bit# 1 is 1, the buffer depth is 2; when bit#2 is 1, the buffer depth is 4, etc. The allowed buffer depth values are 2, 4, 8, 16, 32, 64 and 128.
23:16	**Host CB Write Pointer (H_CBWP)** — RO. Points to next location in the H_CB for host to write the data. Software uses this field along with H_CBRP and H_CBD fields to calculate the number of valid entries in the H_CB to read or number of entries available for write.
15:8	**Host CB Read Pointer (H_CBRP)** — RO. Points to next location in the H_CB where a valid data is available for embedded controller to read. Software uses this field along with H_CBWR and H_CBD fields to calculate the number of valid entries in the host CB to read or number of entries available for write.
7:5	Reserved ***Note:*** For writes to this register, these bits shall be written as 000b.
4	**Host Reset (H_RST)** — R/W. Setting this bit to 1 will initiate a Intel® MEI reset sequence to get the circular buffers into a known good state for host and Intel® ME communication. When this bit transitions from 0 to 1, hardware will clear the H_RDY and ME_RDY bits.
3	**Host Ready (H_RDY)** — R/W. This bit indicates that the host is ready to process messages.
2	**Host Interrupt Generate (H_IG)** — R/W. Once message(s) are written into its CB, the host sets this bit to one for the HW to set the ME_IS bit in the ME_CSR and to generate an interrupt message to Intel® ME. HW will send the interrupt message to Intel ME only if the ME_IE is enabled. HW then clears this bit to 0.

Bit	Description
1	**Host Interrupt Status (H_IS)** — R/WC. Hardware sets this bit to 1 when ME_IG bit is set to 1. Host clears this bit to 0 by writing a 1 to this bit position. H_IE has no effect on this bit.
0	**Host Interrupt Enable (H_IE)** — R/W. Host sets this bit to 1 to enable the host interrupt (INTR# or MSI) to be asserted when H_IS is set to 1.

17.1.2.3 ME_CB_RW—Intel® ME Circular Buffer Read Window Register (Intel® MEI 1 MMIO Register)

Address Offset: MEI0_MBAR + 08h Attribute: RO
Default Value: FFFFFFFFh Size: 32 bits

Bit	Description
31:0	**Intel® ME Circular Buffer Read Window Field (ME_CB_RWF)**. This bit field is for host to read from the Intel® ME Circular Buffer. The Intel® ME's circular buffer is located at the Intel® ME subsystem address specified in the Intel® ME CB Base Address register. This field is read only, writes have no effect. Reads to this register will increment the ME_CBRP as long as ME_RDY is 1. When ME_RDY is 0, reads to this register have no effect, all 1s are returned, and ME_CBRP is not incremented.

17.1.2.4 ME_CSR_HA—Intel® ME Control Status Host Access Register (Intel® MEI 1 MMIO Register)

Address Offset: MEI0_MBAR + 0Ch Attribute: RO
Default Value: 02000000h Size: 32 bits

Bit	Description
31:24	**Intel® ME Circular Buffer Depth Host Read Access (ME_CBD_HRA).** Host read only access to ME_CBD.
23:16	**Intel® ME CB Write Pointer Host Read Access (ME_CBWP_HRA).** Host read only access to ME_CBWP.
15:8	**Intel® ME CB Read Pointer Host Read Access (ME_CBRP_HRA).** Host read only access to ME_CBRP.
7:5	Reserved
4	**Intel® ME Reset Host Read Access (ME_RST_HRA).** Host read access to ME_RST.
3	**Intel® ME Ready Host Read Access (ME_RDY_HRA):** Host read access to ME_RDY.
2	**Intel® ME Interrupt Generate Host Read Access (ME_IG_HRA)**. Host read only access to ME_IG.
1	**Intel® ME Interrupt Status Host Read Access (ME_IS_HRA).** Host read only access to ME_IS.
0	**Intel® ME Interrupt Enable Host Read Access (ME_IE_HRA).** Host read only access to ME_IE.

17.2 Second Intel® Management Engine Interface (Intel® MEI 2) Configuration Registers (Intel® MEI 2—D22:F1)

17.2.1 PCI Configuration Registers (Intel® MEI 2—D22:F2)

Table 17-3. Intel® MEI 2 Configuration Registers Address Map (Intel® MEI 2—D22:F1) (Sheet 1 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
00h–01h	VID	Vendor Identification	8086h	RO
02h–03h	DID	Device Identification	See register description	RO
04h–05h	PCICMD	PCI Command	0000h	R/W, RO
06h–07h	PCISTS	PCI Status	0010h	RO
08h	RID	Revision Identification	See register description	RO
09h–0Bh	CC	Class Code	078000h	RO
0Eh	HTYPE	Header Type	80h	RO
10h–17h	MEI1_MBAR	Intel® MEI 2 MMIO Base Address	0000000000000004h	R/W, RO
2Ch–2Dh	SVID	Subsystem Vendor ID	0000h	R/WO
2Eh–2Fh	SID	Subsystem ID	0000h	R/WO
34h	CAPP	Capabilities List Pointer	50h	RO
3Ch–3Dh	INTR	Interrupt Information	0200h	R/W, RO
40h–43h	HFS	Host Firmware Status	00000000h	RO
48h–4Bh	GMES	General Intel® ME Status	00000000h	RO
4Ch–4Fh	H_GS	Host General Status	00000000h	R/W
50h–51h	PID	PCI Power Management Capability ID	8C01h	RO
52h–53h	PC	PCI Power Management Capabilities	C803h	RO
54h–55h	PMCS	PCI Power Management Control and Status	0008h	R/WC, R/W, RO
60h-63h	GMES2	General Intel® ME Status 2	00000000h	RO
64h-67h	GMES3	General Intel® ME Status 3	00000000h	RO
68h-6Bh	GMES4	General Intel® ME Status 4	00000000h	RO
6Ch-6Fh	GMES5	General Intel® ME Status 5	00000000h	RO
70h-73h	H_GS2	Host General Status 2	00000000h	RW
74h-77h	H_GS3	Host General Status 3	00000000h	RW
8Ch–8Dh	MID	Message Signaled Interrupt Identifiers	0005h	RO
8Eh–8Fh	MC	Message Signaled Interrupt Message Control	0080h	R/W, RO
90h–93h	MA	Message Signaled Interrupt Message Address	00000000h	R/W, RO
94h–97h	MUA	Message Signaled Interrupt Upper Address	00000000h	R/W
98h–99h	MD	Message Signaled Interrupt Message Data	0000h	R/W

Table 17-3. Intel® MEI 2 Configuration Registers Address Map (Intel® MEI 2—D22:F1) (Sheet 2 of 2)

Offset	Mnemonic	Register Name	Default	Attribute
A0h	HIDM	Intel® MEI Interrupt Delivery Mode	00h	R/W
BC–BFh	HERES	Intel® MEI Extended Register Status	40000000h	RO
C0–DFh	HER[1:8]	Intel® MEI Extended Register DW[1:8]	00000000h	RO

17.2.1.1 VID—Vendor Identification Register (Intel® MEI 2—D22:F1)

Address Offset: 00h–01h Attribute: RO
Default Value: 8086h Size: 16 bits

Bit	Description
15:0	**Vendor ID (VID)** — RO. This is a 16-bit value assigned to Intel.

17.2.1.2 DID—Device Identification Register (Intel® MEI 2—D22:F1)

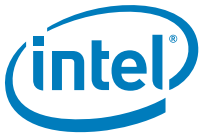
Address Offset: 02h–03h Attribute: RO
Default Value: See bit description Size: 16 bits

Bit	Description
15:0	**Device ID (DID)** — RO. This is a 16-bit value assigned to the Intel® ME Interface controller. See the *Specification Update* for the value of the DID Register.

17.2.1.3 PCICMD—PCI Command Register (Intel® MEI 2—D22:F1)

Address Offset: 04h–05h Attribute: R/W, RO
Default Value: 0000h Size: 16 bits

Bit	Description
15:11	Reserved
10	**Interrupt Disable (ID)** — R/W. Disables this device from generating PCI line based interrupts. This bit does not have any effect on MSI operation.
9:3	Reserved
2	**Bus Master Enable (BME)**— R/W. Controls the Intel® MEI host controller's ability to act as a system memory master for data transfers. When this bit is cleared, Intel® MEI bus master activity stops and any active DMA engines return to an idle condition. This bit is made visible to firmware through the H_PCI_CSR register, and changes to this bit may be configured by the H_PCI_CSR register to generate an Intel® ME MSI. When this bit is 0, Intel® MEI is blocked from generating MSI to the host processor. ***Note:*** This bit does not block Intel® MEI accesses to Intel® ME UMA; that is, writes or reads to the host and Intel® ME circular buffers through the read window and write window registers still cause Intel® ME backbone transactions to Intel® ME UMA.
1	**Memory Space Enable (MSE)** — R/W. Controls access to the Intel® ME's memory mapped register space. 0 = Disable. Memory cycles within the range specified by the memory base and limit registers are master aborted. 1 = Enable. Allows memory cycles within the range specified by the memory base and limit registers accepted.
0	Reserved



17.2.1.4 PCISTS—PCI Status Register (Intel® MEI 2—D22:F1)

Address Offset:	06h–07h	Attribute:	RO
Default Value:	0010h	Size:	16 bits

Bit	Description
15:5	**Reserved**
4	Capabilities List (CL) — RO. Indicates the presence of a capabilities list, hardwired to 1.
3	**Interrupt Status** — RO. Indicates the interrupt status of the device. 0 = Interrupt is deasserted. 1 = Interrupt is asserted.
2:0	Reserved

17.2.1.5 RID—Revision Identification Register (Intel® MEI 2—D22:F1)

Offset Address:	08h	Attribute:	RO
Default Value:	See bit description	Size:	8 bits

Bit	Description
7:0	**Revision ID** — RO. See the *Specification Update* for the value of the RID Register.

17.2.1.6 CC—Class Code Register (Intel® MEI 2—D22:F1)

Address Offset:	09h–0Bh	Attribute:	RO
Default Value:	078000h	Size:	24 bits

Bit	Description
23:16	**Base Class Code (BCC)** — RO. Indicates the base class code of the Intel® MEI device.
15:8	**Sub Class Code (SCC)** — RO. Indicates the sub class code of the Intel® MEI device.
7:0	**Programming Interface (PI)** — RO. Indicates the programming interface of the Intel® MEI device.

17.2.1.7 HTYPE—Header Type Register (Intel® MEI 2—D22:F1)

Address Offset:	0Eh	Attribute:	RO
Default Value:	80h	Size:	8 bits

Bit	Description
7	**Multi-Function Device** (MFD) — RO. Indicates the Intel® MEI host controller is part of a multifunction device.
6:0	**Header Layout (HL)** — RO. Indicates that the Intel® MEI uses a target device layout.

17.2.1.8 MEI1_MBAR—Intel MEI 2 MMIO Base Address (Intel® MEI 2—D22:F1)

Address Offset:	10h–17h	Attribute:	R/W, RO
Default Value:	0000000000000004h	Size:	64 bits

This register allocates space for the Intel® MEI memory mapped registers.

Bit	Description
63:4	**Base Address (BA)** — R/W. Software programs this field with the base address of this region.
3	**Prefetchable Memory (PM)** — RO. Indicates that this range is not pre-fetchable.
2:1	**Type (TP)** — RO. Set to 10b to indicate that this range can be mapped anywhere in 64-bit address space.
0	**Resource Type Indicator (RTE)** — RO. Indicates a request for register memory space.

17.2.1.9 SVID—Subsystem Vendor ID Register (Intel® MEI 2—D22:F1)

Address Offset: 2Ch–2Dh
Default Value: 0000h
Attribute: R/WO
Size: 16 bits

Bit	Description
15:0	**Subsystem Vendor ID (SSVID)** — R/WO. Indicates the sub-system vendor identifier. This field should be programmed by BIOS during boot-up. Once written, this register becomes Read Only. This field can only be cleared by PLTRST#. ***Note:*** Register must be written as a Word write or as a DWord write with SID register.

17.2.1.10 SID—Subsystem ID Register (Intel® MEI 2—D22:F1)

Address Offset: 2Eh–2Fh
Default Value: 0000h
Attribute: R/WO
Size: 16 bits

Bit	Description
15:0	**Subsystem ID (SSID)** — R/WO. Indicates the sub-system identifier. This field should be programmed by BIOS during boot-up. Once written, this register becomes Read Only. This field can only be cleared by PLTRST#. ***Note:*** Register must be written as a Word write or as a DWord write with SVID register.

17.2.1.11 CAPP—Capabilities List Pointer Register (Intel® MEI 2—D22:F1)

Address Offset: 34h
Default Value: 50h
Attribute: RO
Size: 8 bits

Bit	Description
7:0	**Capabilities Pointer (PTR)** — RO. Indicates that the pointer for the first entry in the capabilities list is at 50h in configuration space.

17.2.1.12 INTR—Interrupt Information Register (Intel® MEI 2—D22:F1)

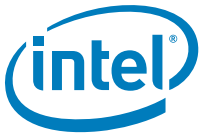
Address Offset: 3Ch–3Dh
Default Value: 0200h
Attribute: R/W, RO
Size: 16 bits

Bit	Description
15:8	**Interrupt Pin (IPIN)** — RO. This field indicates the interrupt pin the Intel MEI host controller uses. A value of 1h/2h/3h/4h indicates that this function implements legacy interrupt on INTA/INTB/INTC/INTD, respectively.
7:0	**Interrupt Line (ILINE)** — R/W. Software written value to indicate which interrupt line (vector) the interrupt is connected to. No hardware action is taken on this register.

17.2.1.13 HFS—Host Firmware Status Register (Intel® MEI 2—D22:F1)

Address Offset: 40h–43h
Default Value: 00000000h
Attribute: RO
Size: 32 bits

Bit	Description
31	**Intel® NM Enabled:** Node Manager power management enabled.
30:12	Reserved
11:9	**SmaRT & CLST Status:** bit 9 – Under-voltage event was noticed at least once since last Intel® ME reset bit 10 – Over-current event was noticed at least once since last Intel® ME reset bit 11 – Over-temperature event was noticed at least once since last Intel® ME reset NOTE: These bits are valid only if bit 31 'NM Enabled' is set.
8	**Power Limiting**: If set to '1' Intel® ME is actively limiting platform power consumption. NOTE: This bit is valid only if bit 31 'NM Enabled' is set.



Bit	Description
7:1	**Cores Disabled**: The number of physical processor cores that should be disabled on each processor socket. NOTE: These bits are valid only if bit 31 'NM Enabled' is set.
0	**BIOS Booting Mode:** This bit is controlled by NM boot time policy. Two modes are supported: 0 – BIOS should run in power optimized mode. 1 –BIOS should run in performance optimized mode (this is the default value when NM is enabled and there is no boot time policy set). NOTE: This bit is valid only if bit 31 'Intel® NM Enabled' is set.

17.2.1.14 GMES—General Intel® ME Status Register (Intel® MEI 2—D22:F1)

Address Offset: 48h–4Bh Attribute: RO
Default Value: 00000000h Size: 32 bits

Bit	Description
31:24	**PTSeqNo:** P/T-state limit request sequence number.
23:0	Reserved

17.2.1.15 H_GS—Host General Status Register (Intel® MEI 2—D22:F1)

Address Offset: 4Ch–4Fh Attribute: R/W
Default Value: 00000000h Size: 32 bits

Bit	Description
31:24	**PTSeqNo:** P/T-state limit request sequence number.
23:0	Reserved

17.2.1.16 PID—PCI Power Management Capability ID Register (Intel® MEI 2—D22:F1)

Address Offset: 50h–51h Attribute: RO
Default Value: 8C01h Size: 16 bits

Bit	Description
15:8	**Next Capability (NEXT)** — RO. Value of 8Ch indicates the location of the next pointer.
7:0	**Capability ID (CID)** — RO. Indicates the linked list item is a PCI Power Management Register.

17.2.1.17 PC—PCI Power Management Capabilities Register (Intel® MEI 2—D22:F1)

Address Offset: 52h–53h Attribute: RO
Default Value: C803h Size: 16 bits

Bit	Description
15:11	**PME_Support (PSUP)** — RO. This five-bit field indicates the power states in which the function may assert PME#. Intel® MEI can assert PME# from any D-state except D1 or D2 which are not supported by Intel® MEI.
10:9	Reserved
8:6	**Aux_Current (AC)** — RO. Reports the maximum Suspend well current required when in the $D3_{cold}$ state. Value of 00b is reported.
5	**Device Specific Initialization (DSI)** — RO. Indicates whether device-specific initialization is required.
4	Reserved
3	**PME Clock (PMEC)** — RO. Indicates that PCI clock is not required to generate PME#.
2:0	**Version (VS)** — RO. Hardwired to 011b to indicate support for *Revision 1.2 of the PCI Power Management Specification*.

17.2.1.18 PMCS—PCI Power Management Control and Status Register (Intel® MEI 2—D22:F1)

Address Offset:	54h–55h	Attribute:	R/WC, R/W, RO
Default Value:	0008h	Size:	16 bits

Bit	Description
15	**PME Status (PMES)** — R/WC. Bit is set by Intel® Server Platform Services FW. Host software clears bit by writing 1 to bit. This bit is reset when CL_RST# is asserted.
14:9	Reserved
8	**PME Enable (PMEE)** — R/W. This bit is read/write and is under the control of host SW. It does not directly have an effect on PME events. However, this bit is shadowed so Intel® Server Platform Services FW can monitor it. Intel® Server Platform Services FW will not cause the PMES bit to transition to 1 while the PMEE bit is 0, indicating that host SW had disabled PME. This bit is reset when PLTRST# asserted.
7:4	Reserved
3	**No_Soft_Reset (NSR)** — RO. This bit indicates that when the Intel® MEI host controller is transitioning from $D3_{hot}$ to D0 due to a power state command, it does not perform an internal reset. Configuration context is preserved.
2	Reserved
1:0	**Power State (PS)** — R/W. This field is used both to determine the current power state of the Intel® MEI host controller and to set a new power state. The values are: 00 = D0 state (default) 11 = $D3_{hot}$ state The D1 and D2 states are not supported for the Intel® MEI host controller. When in the $D3_{hot}$ state, the Intel® ME's configuration space is available, but the register memory spaces are not. Additionally, interrupts are blocked.

17.2.1.19 MID—Message Signaled Interrupt Identifiers Register (Intel® MEI 2—D22:F1)

Address Offset:	8Ch-8Dh	Attribute:	RO
Default Value:	0005h	Size:	16 bits

Bit	Description
15:8	**Next Pointer (NEXT)** — RO. Value of 00h indicates that this is the last item in the list.
7:0	**Capability ID (CID)** — RO. Capabilities ID indicates MSI.

17.2.1.20 MC—Message Signaled Interrupt Message Control Register (Intel® MEI 2—D22:F1)

Address Offset:	8Eh–8Fh	Attribute:	R/W, RO
Default Value:	0080h	Size:	16 bits

Bit	Description
15:8	Reserved
7	**64 Bit Address Capable (C64)** — RO. Specifies that function is capable of generating 64-bit messages.
6:1	Reserved
0	**MSI Enable (MSIE)** — R/W. If set, MSI is enabled and traditional interrupt pins are not used to generate interrupts.

17.2.1.21 MA—Message Signaled Interrupt Message Address Register (Intel® MEI 2—D22:F1)

Address Offset:	90h–93h	Attribute:	R/W, RO
Default Value:	00000000h	Size:	32 bits

Bit	Description
31:2	**Address (ADDR)** — R/W. Lower 32 bits of the system specified message address, always DW aligned.
1:0	Reserved

17.2.1.22 MUA—Message Signaled Interrupt Upper Address Register (Intel® MEI 2—D22:F1)

Address Offset:	94h–97h	Attribute:	R/W
Default Value:	00000000h	Size:	32 bits

Bit	Description
31:0	**Upper Address (UADDR)** — R/W. Upper 32 bits of the system specified message address, always DW aligned.

17.2.1.23 MD—Message Signaled Interrupt Message Data Register (Intel® MEI 2—D22:F1)

Address Offset:	98h–99h	Attribute:	R/W
Default Value:	0000h	Size:	16 bits

Bit	Description
15:0	**Data (DATA)** — R/W. This 16-bit field is programmed by system software if MSI is enabled. Its content is driven during the data phase of the MSI memory write transaction.

17.2.1.24 HIDM—Intel® MEI Interrupt Delivery Mode Register (Intel® MEI 2—D22:F1)

Address Offset:	A0h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

Bit	Description
7:2	Reserved
1:0	**Intel® MEI Interrupt Delivery Mode (HIDM)** — R/W. These bits control what type of interrupt the Intel® MEI will send the host. They are interpreted as follows: 00 = Generate Legacy or MSI interrupt 01 = Generate SCI 10 = Generate SMI

17.2.1.25 HERES—Intel® MEI Extend Register Status (Intel® MEI 2—D22:F1)

Address Offset:	BCh–BFh	Attribute:	RO
Default Value:		Size:	32 bits

Bit	Description
31	**Extend Register Valid (ERV)**- RO. Set by firmware after all firmware has been loaded. If ERA field is SHA-1, the result of the extend operation is in HER:5-1. If ERA field is SHA-256, the result of the extend operation is in HER:8-1.
30	**Extend Feature Present (EFP)- RO.** This bit is hardwired to 1 to allow driver software to easily detect the chipset supports the Extend Register FW measurement feature.
29:4	Reserved

Bit	Description
3:0	**Extend Register Algorithm (ERA)- RO.** This field indicates the hash algorithm used in the FW measurement extend operations. Encodings are: 0h = SHA-1 2h = SHA-256 Other values = Reserved

17.2.1.26 HERX—Intel® MEI Extend Register DWX (Intel® MEI 2—D22:F1)

Address Offset: HER1: C0h–C3h
HER2: C4h–C7h
HER3: C8h–CBh
HER4: CCh–CFh
HER5: D0h–D3h
HER6: D4h–D7h
HER7: D8h–DBh
HER8: DCh–DFh — Attribute: RO

Default Value: 00000000h — Size: 32 bits

Bit	Description
31:0	Extend Register DWX (ERDWX): Xth DWORD result of the extend operation. ***Note:*** Extend Operation is HER[5:1] if using SHA-1. If using SHA-256, then Extend Operation is HER[8:1].

17.2.2 MEI1_MBAR—Intel® MEI 2 MMIO Registers

These MMIO registers are accessible starting at the Intel® MEI 2 MMIO Base Address (MEI1_MBAR) which gets programmed into D22:F1:Offset 10–17h. These registers are reset by PLTRST# unless otherwise noted.

Table 17-4. Intel® MEI 2 MMIO Register Address Map

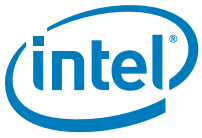
MEI1_MBAR+ Offset	Mnemonic	Register Name	Default	Attribute
00–03h	H_CB_WW	Host Circular Buffer Write Window	00000000h	W
04h–07h	H_CSR	Host Control Status	02000000h	R/W, R/WC, RO
08h–0Bh	ME_CB_RW	Intel® ME Circular Buffer Read Window	FFFFFFFFh	RO
0Ch–0Fh	ME_CSR_HA	Intel® ME Control Status Host Access	02000000h	RO

17.2.2.1 H_CB_WW—Host Circular Buffer Write Window (Intel® MEI 2 MMIO Register)

Address Offset: MEI1_MBAR + 00h — Attribute: W

Default Value: 00000000h — Size: 32 bits

Bit	Description
31:0	**Host Circular Buffer Write Window Field (H_CB_WWF)- W.** This bit field is for host to write into its circular buffer. The host's circular buffer is located at the Intel® ME subsystem address specified in the Host CB Base Address register. This field is write only, reads will return arbitrary data. Writes to this register will increment the H_CBWP as long as ME_RDY is 1. When ME_RDY is 0, writes to this register have no effect and are not delivered to the H_CB, nor is H_CBWP incremented.



17.2.2.2 H_CSR—Host Control Status Register (Intel® MEI 2 MMIO Register)

Address Offset:	MEI1_MBAR + 04h	Attribute:	RO, R/W, R/WC
Default Value:	02000000h	Size:	32 bits

Bit	Description
31:24	**Host Circular Buffer Depth (H_CBD)** — RO. This field indicates the maximum number of 32 bit entries available in the host circular buffer (H_CB). Host software uses this field along with the H_CBRP and H_CBWP fields to calculate the number of valid entries in the H_CB to read or # of entries available for write. This field is implemented with a "1-hot" scheme. Only one bit will be set to a "1" at a time. Each bit position represents the value n of a buffer depth of (2^n). For example, when bit# 1 is 1, the buffer depth is 2; when bit#2 is 1, the buffer depth is 4, etc. The allowed buffer depth values are 2, 4, 8, 16, 32, 64 and 128.
23:16	**Host CB Write Pointer (H_CBWP)** — RO. Points to next location in the H_CB for host to write the data. Software uses this field along with H_CBRP and H_CBD fields to calculate the number of valid entries in the H_CB to read or number of entries available for write.
15:8	**Host CB Read Pointer (H_CBRP)** — RO. Points to next location in the H_CB where a valid data is available for embedded controller to read. Software uses this field along with H_CBWR and H_CBD fields to calculate the number of valid entries in the host CB to read or number of entries available for write.
7:5	Reserved ***Note:*** For writes to this register, these bits shall be written as 000b.
4	**Host Reset (H_RST)** — R/W. Setting this bit to 1 will initiate a Intel® MEI reset sequence to get the circular buffers into a known good state for host and Intel® ME communication. When this bit transitions from 0 to 1, hardware will clear the H_RDY and ME_RDY bits.
3	**Host Ready (H_RDY)** — R/W. This bit indicates that the host is ready to process messages.
2	**Host Interrupt Generate (H_IG)** — R/W. Once message(s) are written into its CB, the host sets this bit to one for the HW to set the ME_IS bit in the ME_CSR and to generate an interrupt message to Intel® ME. HW will send the interrupt message to Intel® ME only if the ME_IE is enabled. HW then clears this bit to 0.
1	**Host Interrupt Status (H_IS)** — R/WC. Hardware sets this bit to 1 when ME_IG bit is set to 1. Host clears this bit to 0 by writing a 1 to this bit position. H_IE has no effect on this bit.
0	**Host Interrupt Enable (H_IE)** — R/W. Host sets this bit to 1 to enable the host interrupt (INTR# or MSI) to be asserted when H_IS is set to 1.

17.2.2.3 ME_CB_RW—Intel® ME Circular Buffer Read Window Register (Intel® MEI 2 MMIO Register)

Address Offset:	MEI1_MBAR + 08h	Attribute:	RO
Default Value:	FFFFFFFFh	Size:	32 bits

Bit	Description
31:0	**Intel® ME Circular Buffer Read Window Field (ME_CB_RWF)**. This bit field is for host to read from the Intel® ME Circular Buffer. The Intel® ME's circular buffer is located at the Intel® ME subsystem address specified in the Intel® ME CB Base Address register. This field is read only, writes have no effect. Reads to this register will increment the ME_CBRP as long as ME_RDY is 1. When ME_RDY is 0, reads to this register have no effect, all 1s are returned, and ME_CBRP is not incremented.

17.2.2.4 ME_CSR_HA—Intel® ME Control Status Host Access Register (Intel® MEI 2 MMIO Register)

Address Offset: MEI1_MBAR + 0Ch
Attribute: RO
Default Value: 02000000h
Size: 32 bits

Bit	Description
31:24	Intel® ME Circular Buffer Depth Host Read Access (ME_CBD_HRA). Host read only access to ME_CBD.
23:16	Intel® ME CB Write Pointer Host Read Access (ME_CBWP_HRA). Host read only access to ME_CBWP.
15:8	Intel® ME CB Read Pointer Host Read Access (ME_CBRP_HRA). Host read only access to ME_CBRP.
7:5	Reserved
4	Intel® ME Reset Host Read Access (ME_RST_HRA). Host read access to ME_RST.
3	Intel® ME Ready Host Read Access (ME_RDY_HRA). Host read access to ME_RDY.
2	Intel® ME Interrupt Generate Host Read Access (ME_IG_HRA). Host read only access to ME_IG.
1	Intel® ME Interrupt Status Host Read Access (ME_IS_HRA). Host read only access to ME_IS.
0	Intel® ME Interrupt Enable Host Read Access (ME_IE_HRA). Host read only access to ME_IE.

17.3 IDE Redirect IDER Registers (IDER — D22:F2)

17.3.1 PCI Configuration Registers (IDER—D22:F2)

Table 17-5. IDE Redirect Function IDER Register Address Map (Sheet 1 of 2)

Address Offset	Register Symbol	Register Name	Default Value	Attribute
00h–01h	VID	Vendor Identification	8086h	RO
02h–03h	DID	Device Identification	See register description	RO
04h–05h	PCICMD	PCI Command	0000h	RO, R/W
06h–07h	PCISTS	PCI Status	00B0h	RO
08h	RID	Revision ID	See register description	RO
09h–0Bh	CC	Class Codes	010185h	RO
0Ch	CLS	Cache Line Size	00h	RO
10h–13h	PCMDBA	Primary Command Block IO Bar	00000001h	RO, R/W
14h–17h	PCTLBA	Primary Control Block Base Address	00000001h	RO, R/W
18h–1Bh	SCMDBA	Secondary Command Block Base Address	00000001h	RO, R/W
1Ch–1Fh	SCTLBA	Secondary Control Block base Address	00000001h	RO, R/W
20h–23h	LBAR	Legacy Bus Master Base Address	00000001h	RO, R/W
2Ch–2Dh	SVID	Subsystem Vendor ID	0000h	R/WO
2Eh–2Fh	SID	Subsystem ID	8086h	R/WO
34h	CAPP	Capabilities Pointer	C8h	RO
3Ch–3Dh	INTR	Interrupt Information	0300h	R/W, RO

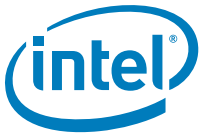


Table 17-5. IDE Redirect Function IDER Register Address Map (Sheet 2 of 2)

Address Offset	Register Symbol	Register Name	Default Value	Attribute
C8h–C9h	PID	PCI Power Management Capability ID	D001h	RO
CAh–CBh	PC	PCI Power Management Capabilities	0023h	RO
CCh–CFh	PMCS	PCI Power Management Control and Status	00000000h	RO, R/W, RO/V
D0h–D1h	MID	Message Signaled Interrupt Capability ID	0005h	RO
D2h–D3h	MC	Message Signaled Interrupt Message Control	0080h	RO, R/W
D4h–D7h	MA	Message Signaled Interrupt Message Address	00000000h	R/W, RO
D8h–DBh	MAU	Message Signaled Interrupt Message Upper Address	00000000h	RO, R/W
DC–DDh	MD	Message Signaled Interrupt Message Data	0000h	R/W

17.3.1.1 VID—Vendor Identification Register (IDER—D22:F2)

Address Offset: 00–01h
Default Value: 8086h
Attribute: RO
Size: 16 bits

Bit	Description
15:0	**Vendor ID (VID)** — RO. This is a 16-bit value assigned by Intel.

17.3.1.2 DID—Device Identification Register (IDER—D22:F2)

Address Offset: 02–03h
Default Value: See bit description
Attribute: RO
Size: 16 bits

Bit	Description
15:0	**Device ID (DID)** — RO. This is a 16-bit value assigned to the Intel® Xeon® Processor D-1500 Product Family IDER controller. See the *Specification Update* for the value of the DID Register.

17.3.1.3 PCICMD— PCI Command Register (IDER—D22:F2)

Address Offset: 04–05h
Default Value: 0000h
Attribute: RO, R/W
Size: 16 bits

Bit	Description
15:11	Reserved
10	**Interrupt Disable (ID)**—R/W**.** This disables pin-based INTx# interrupts. This bit has no effect on MSI operation. When set, internal INTx# messages will not be generated. When cleared, internal INTx# messages are generated if there is an interrupt **and** MSI is not enabled.
9:3	**Reserved**
2	**Bus Master Enable (BME)**—RO. This bit controls the PT function's ability to act as a master for data transfers. This bit does not impact the generation of completions for split transaction commands.
1	**Memory Space Enable (MSE)**—RO. PT function does not contain target memory space.
0	**I/O Space enable (IOSE)**—RO. This bit controls access to the PT function's target I/O space.

17.3.1.4 PCISTS—PCI Device Status Register (IDER—D22:F2)

Address Offset: 06–07h Attribute: RO
Default Value: 00B0h Size: 16 bits

Bit	Description
15:11	Reserved
10:9	**DEVSEL# Timing Status (DEVT)**—RO. This bit controls the device select time for the PT function's PCI interface.
8:5	Reserved
4	**Capabilities List (CL)**—RO. This bit indicates that there is a capabilities pointer implemented in the device.
3	**Interrupt Status (IS)**—RO. This bit reflects the state of the interrupt in the function. Setting of the Interrupt Disable bit to 1 has no affect on this bit. Only when this bit is a 1 and ID bit is 0 is the INTc interrupt asserted to the Host.
2:0	Reserved

17.3.1.5 RID—Revision Identification Register (IDER—D22:F2)

Address Offset: 08h Attribute: RO
Default Value: See bit description Size: 8 bits

Bit	Description
7:0	**Revision ID** — RO. See the *Specification Update* for the value of the RID Register.

17.3.1.6 CC—Class Codes Register (IDER—D22:F2)

Address Offset: 09–0Bh Attribute: RO
Default Value: 010185h Size: 24 bits

Bit	Description
23:16	**Base Class Code (BCC)**—RO This field indicates the base class code of the IDER host controller device.
15:8	**Sub Class Code (SCC)**—RO This field indicates the sub class code of the IDER host controller device.
7:0	**Programming Interface (PI)**—RO This field indicates the programming interface of the IDER host controller device.

17.3.1.7 CLS—Cache Line Size Register (IDER—D22:F2)

Address Offset: 0Ch Attribute: RO
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Cache Line Size (CLS)**—RO. All writes to system memory are Memory Writes.

17.3.1.8 PCMDBA—Primary Command Block IO Bar Register (IDER—D22:F2)

Address Offset: 10–13h
Default Value: 00000001h
Attribute: RO, R/W
Size: 32 bits

Bit	Description
31:16	Reserved
15:3	**Base Address (BAR)**—R/W Base Address of the BAR0 I/O space (8 consecutive I/O locations).
2:1	Reserved
0	**Resource Type Indicator (RTE)**—RO. This bit indicates a request for I/O space.

17.3.1.9 PCTLBA—Primary Control Block Base Address Register (IDER—D22:F2)

Address Offset: 14–17h
Default Value: 00000001h
Attribute: RO, R/W
Size: 32 bits

Bit	Description
31:16	Reserved
15:2	**Base Address (BAR)**—R/W. Base Address of the BAR1 I/O space (4 consecutive I/O locations)
1	Reserved
0	**Resource Type Indicator (RTE)**—RO. This bit indicates a request for I/O space

17.3.1.10 SCMDBA—Secondary Command Block Base Address Register (IDER—D22:F2)

Address Offset: 18–1Bh
Default Value: 00000001h
Attribute: RO, R/W
Size: 32 bits

Bit	Description
31:16	Reserved
15:3	**Base Address (BAR)**—R/W. Base Address of the I/O space (8 consecutive I/O locations).
2:1	Reserved
0	**Resource Type Indicator (RTE)**—RO. This bit indicates a request for I/O space.

17.3.1.11 SCTLBA—Secondary Control Block Base Address Register (IDER—D22:F2)

Address Offset: 1C–1Fh
Default Value: 00000001h
Attribute: RO, R/W
Size: 32 bits

Bit	Description
31:16	Reserved
15:2	**Base Address (BAR)**—R/W. Base Address of the I/O space (4 consecutive I/O locations).
1	Reserved
0	**Resource Type Indicator (RTE)**—RO. This bit indicates a request for I/O space.

17.3.1.12 LBAR—Legacy Bus Master Base Address Register (IDER—D22:F2)

Address Offset: 20–23h Attribute: RO, R/W
Default Value: 00000001h Size: 32 bits

Bit	Description
31:16	Reserved
15:4	**Base Address (BA)**—R/W. Base Address of the I/O space (16 consecutive I/O locations).
3:1	Reserved
0	**Resource Type Indicator (RTE)**—RO. This bit indicates a request for I/O space.

17.3.1.13 SVID—Subsystem Vendor ID Register (IDER—D22:F2)

Address Offset: 2Ch–2Dh Attribute: R/WO
Default Value: 0000h Size: 16 bits

Bit	Description
15:0	**Subsystem Vendor ID (SSVID)** — R/WO. Indicates the sub-system vendor identifier. This field should be programmed by BIOS during boot-up. Once written, this register becomes Read Only. This field can only be cleared by PLTRST#. ***Note:*** Register must be written as a DWord write with SID register.

17.3.1.14 SID—Subsystem ID Register (IDER—D22:F2)

Address Offset: 2Eh–2Fh Attribute: R/WO
Default Value: 8086h Size: 16 bits

Bit	Description
15:0	**Subsystem ID (SSID)** — R/WO. Indicates the sub-system identifier. This field should be programmed by BIOS during boot-up. Once written, this register becomes Read Only. This field can only be cleared by PLTRST#. ***Note:*** Register must be written as a DWord write with SVID register.

17.3.1.15 CAPP—Capabilities List Pointer Register (IDER—D22:F2)

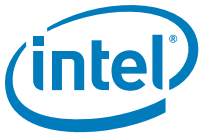
Address Offset: 34h Attribute: RO
Default Value: C8h Size: 8 bits

Bit	Description
7:0	**Capability Pointer (CP)**— R/WO. This field indicates that the first capability pointer is offset C8h (the power management capability).

17.3.1.16 INTR—Interrupt Information Register (IDER—D22:F2)

Address Offset: 3C–3Dh Attribute: R/W, RO
Default Value: 0300h Size: 16 bits

Bit	Description
15:8	**Interrupt Pin (IPIN)** — RO. A value of 1h/2h/3h/4h indicates that this function implements legacy interrupt on INTA/INTB/INTC/INTD, respectively FunctionValueINTx (2 IDE)03hINTC
7:0	**Interrupt Line (ILINE)**— R/W. The value written in this register indicates which input of the system interrupt controller, the device's interrupt pin is connected to. This value is used by the OS and the device driver, and has no affect on the hardware.



17.3.1.17 PID—PCI Power Management Capability ID Register (IDER—D22:F2)

Address Offset: C8–C9h
Default Value: D001h
Attribute: RO
Size: 16 bits

Bit	Description
15:8	**Next Capability (NEXT)** — RO. Its value of D0h points to the MSI capability.
7:0	**Cap ID (CID)**— RO. This field indicates that this pointer is a PCI power management.

17.3.1.18 PC—PCI Power Management Capabilities Register (IDER—D22:F2)

Address Offset: CA–CBh
Default Value: 0023h
Attribute: RO
Size: 16 bits

Bit	Description
15:11	**PME_Support (PSUP)** — RO. This five-bit field indicates the power states in which the function may assert PME#. IDER can assert PME# from any D-state except D1 or D2 which are not supported by IDER.
10:9	Reserved
8:6	**Aux_Current (AC)** — RO. Reports the maximum Suspend well current required when in the $D3_{cold}$ state. Value of 000b is reported.
5	**Device Specific Initialization (DSI)** — RO. Indicates whether device-specific initialization is required.
4	Reserved
3	**PME Clock (PMEC)** — RO. Indicates that PCI clock is not required to generate PME#.
2:0	**Version (VS)** — RO. Hardwired to 011b to indicate support for *Revision 1.2 of the PCI Power Management Specification*.

17.3.1.19 PMCS—PCI Power Management Control and Status Register (IDER—D22:F2)

Address Offset: CC-CFh
Default Value: 00000000h
Attribute: RO, R/W
Size: 32 bits

Bit	Description
31:4	Reserved
3	**No Soft Reset (NSR)** — RO. 0 = Devices do perform an internal reset upon transitioning from D3hot to D0 using software control of the PowerState bits. Configuration Context is lost when performing the soft reset. Upon transition from the D3hot to the D0 state, full re-initialization sequence is needed to return the device to D0 Initialized. 1 = Devices do not perform an internal reset upon transitioning from D3hot to D0. Configuration Context is preserved. Upon transition from the D3hot to the D0 Initialized state, no additional operating system intervention is required to preserve Configuration Context beyond writing the PowerState bits.
2	Reserved
1:0	**Power State (PS)**— R/W. This field is used both to determine the current power state of the PT function and to set a new power state. The values are: 00 = D0 state 11 = $D3_{HOT}$ state When in the $D3_{HOT}$ state, the controller's configuration space is available, but the I/O and memory spaces are not. Additionally, interrupts are blocked. If software attempts to write a '10' or '01' to these bits, the write will be ignored.

17.3.1.20 MID—Message Signaled Interrupt Capability ID Register (IDER—D22:F2)

Address Offset: D0–D1h
Default Value: 0005h
Attribute: RO
Size: 16 bits

Bit	Description
15:8	**Next Pointer (NEXT)** — RO. This value indicates this is the last item in the capabilities list.
7:0	**Capability ID (CID)** — RO. The Capabilities ID value indicates device is capable of generating an MSI.

17.3.1.21 MC—Message Signaled Interrupt Message Control Register (IDER—D22:F2)

Address Offset: D2–D3h
Default Value: 0080h
Attribute: RO, R/W
Size: 16 bits

Bit	Description
15:8	Reserved
7	**64-Bit Address Capable (C64)** — RO. Capable of generating 64-bit and 32-bit messages.
6:4	**Multiple Message Enable (MME)** — R/W. These bits are R/W for software compatibility, but only one message is ever sent by the PT function.
3:1	**Multiple Message Capable (MMC)** — RO. Only one message is required.
0	**MSI Enable (MSIE)** — R/W. If set, MSI is enabled and traditional interrupt pins are not used to generate interrupts.

17.3.1.22 MA—Message Signaled Interrupt Message Address Register (IDER—D22:F2)

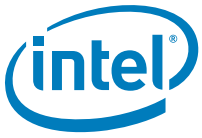
Address Offset: D4–D7h
Default Value: 00000000h
Attribute: R/W, RO
Size: 32 bits

Bit	Description
31:2	**Address (ADDR)** — R/W. This field contains the Lower 32 bits of the system specified message address, always DWord aligned
1:0	Reserved

17.3.1.23 MAU—Message Signaled Interrupt Message Upper Address Register (IDER—D22:F2)

Address Offset: D8–DBh
Default Value: 00000000h
Attribute: RO, R/W
Size: 32 bits

Bit	Description
31:4	Reserved
3:0	**Address (ADDR)** — R/W. This field contains the Upper 4 bits of the system specified message address.



17.3.1.24 MD—Message Signaled Interrupt Message Data Register (IDER—D22:F2)

Address Offset:	DC–DDh	Attribute:	R/W
Default Value:	0000h	Size:	16 bits

Bit	Description
15:0	**Data (DATA)** — R/W. This content is driven onto the lower word of the data bus of the MSI memory write transaction.

17.3.2 IDER BAR0 Registers

Table 17-6. IDER BAR0 Register Address Map

Address Offset	Register Symbol	Register Name	Default Value	Attribute
0h	IDEDATA	IDE Data Register	00h	R/W
1h	IDEERD1	IDE Error Register DEV1	00h	R/W
1h	IDEERD0	IDE Error Register DEV0	00h	R/W
1h	IDEFR	IDE Features Register	00h	R/W
2h	IDESCIR	IDE Sector Count In Register	00h	R/W
2h	IDESCOR1	IDE Sector Count Out Register Device 1	00h	R/W
2h	IDESCOR0	IDE Sector Count Out Register Device 0	00h	R/W
3h	IDESNOR0	IDE Sector Number Out Register Device 0	00h	R/W
3h	IDESNOR1	IDE Sector Number Out Register Device 1	00h	R/W
3h	IDESNIR	IDE Sector Number In Register	00h	R/W
4h	IDECLIR	IDE Cylinder Low In Register	00h	R/W
4h	IDCLOR1	IDE Cylinder Low Out Register Device 1	00h	R/W
4h	IDCLOR0	IDE Cylinder Low Out Register Device 0	00h	R/W
5h	IDCHOR0	IDE Cylinder High Out Register Device 0	00h	R/W
5h	IDCHOR1	IDE Cylinder High Out Register Device 1	00h	R/W
5h	IDECHIR	IDE Cylinder High In Register	00h	R/W
6h	IDEDHIR	IDE Drive/Head In Register	00h	R/W
6h	IDDHOR1	IDE Drive Head Out Register Device 1	00h	R/W
6h	IDDHOR0	IDE Drive Head Out Register Device 0	00h	R/W
7h	IDESD0R	IDE Status Device 0 Register	80h	R/W
7h	IDESD1R	IDE Status Device 1 Register	80h	R/W
7h	IDECR	IDE Command Register	00h	R/W

17.3.2.1 IDEDATA—IDE Data Register (IDER—D22:F2)

Address Offset:	0h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

The IDE data interface is a special interface that is implemented in the HW. This data interface is mapped to I/O space from the host and takes read and write cycles from the host targeting master or slave device.

Writes from host to this register result in the data being written to Intel® ME memory.

Reads from host to this register result in the data being fetched from Intel® ME memory.

Data is typically written/ read in WORDs. Intel® Server Platform Services FW must enable hardware to allow it to accept Host initiated Read/ Write cycles, else the cycles are dropped.

Bit	Description
7:0	**IDE Data Register (IDEDR)** — R/W. Data Register implements the data interface for IDE. All writes and reads to this register translate into one or more corresponding write/reads to Intel® ME memory.

17.3.2.2 IDEERD1—IDE Error Register DEV1 (IDER—D22:F2)

Address Offset: 01h
Default Value: 00h
Attribute: R/W
Size: 8 bits

This register implements the Error register of the command block of the IDE function. This register is read only by the HOST interface when DEV = 1 (slave device).

Bit	Description
7:0	**IDE Error Data (IDEED)** — R/W. Drive reflects its error/ diagnostic code to the host using this register at different times.

17.3.2.3 IDEERD0—IDE Error Register DEV0 (IDER—D22:F2)

Address Offset: 01h
Default Value: 00h
Attribute: R/W
Size: 8 bits

This register implements the Error register of the command block of the IDE function. This register is read only by the HOST interface when DEV = 0 (master device).

Bit	Description
7:0	**IDE Error Data (IDEED)**— R/W. Drive reflects its error/ diagnostic code to the host using this register at different times.

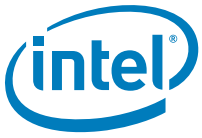
17.3.2.4 IDEFR—IDE Features Register (IDER—D22:F2)

Address Offset: 01h
Default Value: 00h
Attribute: R/W
Size: 8 bits

This register implements the Feature register of the command block of the IDE function. This register can be written only by the Host.

When the HOST reads the same address, it reads the Error register of Device 0 or Device 1 depending on the device_select bit (bit 4 of the drive/head register).

Bit	Description
7:0	**IDE Feature Data (IDEFD)** — R/W. IDE drive specific data written by the Host



17.3.2.5 IDESCIR—IDE Sector Count In Register (IDER—D22:F2)

Address Offset:	02h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register implements the Sector Count register of the command block of the IDE function. This register can be written only by the Host. When host writes to this register, all 3 registers (IDESCIR, IDESCOR0, IDESCOR1) are updated with the written value.

A host read to this register address reads the IDE Sector Count Out Register IDESCOR0 if DEV=0 or IDESCOR1 if DEV=1

Bit	Description
7:0	**IDE Sector Count Data (IDESCD)**— R/W. Host writes the number of sectors to be read or written.

17.3.2.6 IDESCOR1—IDE Sector Count Out Register Device 1 Register (IDER—D22:F2)

Address Offset:	02h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register is read by the HOST interface if DEV = 1. Intel® Server Platform Services Firmware writes to this register at the end of a command of the selected device.

When the host writes to this address, the IDE Sector Count In Register (IDESCIR), this register is updated.

Bit	Description
7:0	**IDE Sector Count Out Dev1 (ISCOD1)** — R/W. Sector Count register for Slave Device (that is, Device 1)

17.3.2.7 IDESCOR0—IDE Sector Count Out Register Device 0 Register (IDER—D22:F2)

Address Offset:	02h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register is read by the HOST interface if DEV = 0. Intel® Server Platform Services Firmware writes to this register at the end of a command of the selected device.

When the host writes to this address, the IDE Sector Count In Register (IDESCIR), this register is updated.

Bit	Description
7:0	**IDE Sector Count Out Dev0 (ISCOD0)** — R/W. Sector Count register for Master Device (that is, Device 0).

17.3.2.8 IDESNOR0—IDE Sector Number Out Register Device 0 Register (IDER—D22:F2)

Address Offset:	03h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register is read by the Host if DEV = 0. Intel® Server Platform Services Firmware writes to this register at the end of a command of the selected device.

When the host writes to the IDE Sector Number In Register (IDESNIR), this register is updated with that value.

Bit	Description
7:0	**IDE Sector Number Out DEV 0 (IDESNO0)** — R/W. Sector Number Out register for Master device.

17.3.2.9 IDESNOR1—IDE Sector Number Out Register Device 1 Register (IDER—D22:F2)

Address Offset:	03h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register is read by the Host if DEV = 1. Intel® Server Platform Services Firmware writes to this register at the end of a command of the selected device.

When the host writes to the IDE Sector Number In Register (IDESNIR), this register is updated with that value.

Bit	Description
7:0	**IDE Sector Number Out DEV 1 (IDESNO1)** — R/W. Sector Number Out register for Slave device.

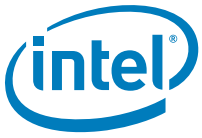
17.3.2.10 IDESNIR—IDE Sector Number In Register (IDER—D22:F2)

Address Offset:	03h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register implements the Sector Number register of the command block of the IDE function. This register can be written only by the Host. When host writes to this register, all 3 registers (IDESNIR, IDESNOR0, IDESNOR1) are updated with the written value.

Host read to this register address reads the IDE Sector Number Out Register IDESNOR0 if DEV=0 or IDESNOR1 if DEV=1.

Bit	Description
7:0	**IDE Sector Number Data (IDESND)** — R/W. This register contains the number of the first sector to be transferred.



17.3.2.11 IDECLIR—IDE Cylinder Low In Register (IDER—D22:F2)

Address Offset:	04h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register implements the Cylinder Low register of the command block of the IDE function. This register can be written only by the Host. When host writes to this register, all 3 registers (IDECLIR, IDECLOR0, IDECLOR1) are updated with the written value.

Host read to this register address reads the IDE Cylinder Low Out Register IDECLOR0 if DEV=0 or IDECLOR1 if DEV=1.

Bit	Description
7:0	**IDE Cylinder Low Data (IDECLD)** — R/W. Cylinder Low register of the command block of the IDE function.

17.3.2.12 IDCLOR1—IDE Cylinder Low Out Register Device 1 Register (IDER—D22:F2)

Address Offset:	04h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register is read by the Host if DEV = 1. Intel® Server Platform Services Firmware writes to this register at the end of a command of the selected device. When the host writes to the IDE Cylinder Low In Register (IDECLIR), this register is updated with that value.

Bit	Description
7:0	**IDE Cylinder Low Out DEV 1. (IDECLO1)** — R/W. Cylinder Low Out Register for Slave Device.

17.3.2.13 IDCLOR0—IDE Cylinder Low Out Register Device 0 Register (IDER—D22:F2)

Address Offset:	04h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register is read by the Host if DEV = 0. Intel® Server Platform Services Firmware writes to this register at the end of a command of the selected device. When the host writes to the IDE Cylinder Low In Register (IDECLIR), this register is updated with that value.

Bit	Description
7:0	**IDE Cylinder Low Out DEV 0. (IDECLO0)** — R/W. Cylinder Low Out Register for Master Device.

17.3.2.14 IDCHOR0—IDE Cylinder High Out Register Device 0 Register (IDER—D22:F2)

Address Offset:	05h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register is read by the Host if Device = 0. Intel® Server Platform Services Firmware writes to this register at the end of a command of the selected device. When the host writes to the IDE Cylinder High In Register (IDECHIR), this register is updated with that value.

Bit	Description
7:0	**IDE Cylinder High Out DEV 0 (IDECHO0)** — R/W. Cylinder High out register for Master device.

17.3.2.15 IDCHOR1—IDE Cylinder High Out Register Device 1 Register (IDER—D22:F2)

Address Offset:	05h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register is read by the Host if Device = 1. Intel® Server Platform Services Firmware writes to this register at the end of a command of the selected device. When the host writes to the IDE Cylinder High In Register (IDECHIR), this register is updated with that value.

Bit	Description
7:0	**IDE Cylinder High Out DEV 1 (IDECHO1)** — R/W. Cylinder High out register for Slave device.

17.3.2.16 IDECHIR—IDE Cylinder High In Register (IDER—D22:F2)

Address Offset:	05h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register implements the Cylinder High register of the command block of the IDE function. This register can be written only by the Host. When host writes to this register, all 3 registers (IDECHIR, IDECHOR0, IDECHOR1) are updated with the written value.

Host read to this register address reads the IDE Cylinder High Out Register IDECHOR0 if DEV=0 or IDECHOR1 if DEV=1.

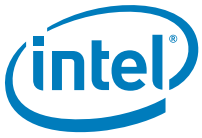
Bit	Description
7:0	**IDE Cylinder High Data (IDECHD)** — R/W. Cylinder High data register for IDE command block.

17.3.2.17 IDEDHIR—IDE Drive/Head In Register (IDER—D22:F2)

Address Offset:	06h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register implements the Drive/Head register of the command block of the IDE. This register can be written only by the Host. When host writes to this register, all 3 registers (IDEDHIR, IDEDHOR0, IDEDHOR1) are updated with the written value.

Host read to this register address reads the IDE Drive/Head Out Register (IDEDHOR0) if DEV=0 or IDEDHOR1 if DEV=1.



Bit 4 of this register is the DEV (master/slave) bit. This bit is cleared by hardware on IDE software reset (S_RST toggles to '1') in addition to Host system reset and D3->D0 transition of the function.

Bit	Description
7:0	**IDE Drive/Head Data (IDEDHD)** — R/W. Register defines the drive number, head number and addressing mode.

17.3.2.18 IDDHOR1—IDE Drive Head Out Register Device 1 Register (IDER—D22:F2)

Address Offset:	06h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register is read only by the Host. Host read to this Drive/head In register address reads the IDE Drive/Head Out Register (IDEDHOR0) if DEV=1

Bit 4 of this register is the DEV (master/slave) bit. This bit is cleared by hardware on IDE software reset (S_RST toggles to '1') in addition to the Host system reset and D3 to D0 transition of the IDE function.

When the host writes to this address, it updates the value of the IDEDHIR register.

Bit	Description
7:0	**IDE Drive Head Out DEV 1 (IDEDHO1)** — R/W. Drive/Head Out register of Slave device.

17.3.2.19 IDDHOR0—IDE Drive Head Out Register Device 0 Register (IDER—D22:F2)

Address Offset:	06h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register is read only by the Host. Host read to this Drive/head In register address reads the IDE Drive/Head Out Register (IDEDHOR0) if DEV=0.

Bit 4 of this register is the DEV (master/slave) bit. This bit is cleared by hardware on IDE software reset (S_RST toggles to 1) in addition to the Host system reset and D3 to D0 transition of the IDE function.

When the host writes to this address, it updates the value of the IDEDHIR register.

Bit	Description
7:0	**IDE Drive Head Out DEV 0 (IDEDHO0)** — R/W. Drive/Head Out register of Master device.

17.3.2.20 IDESD0R—IDE Status Device 0 Register (IDER—D22:F2)

Address Offset:	07h	Attribute:	R/W
Default Value:	80h	Size:	8 bits

This register implements the status register of the Master device (DEV = 0). This register is read only by the Host. Host read of this register clears the Master device's interrupt.

When the HOST writes to the same address it writes to the command register

The bits description is for ATA mode.

Bit	Description
7	**Busy (BSY)** — R/W. This bit is set by HW when the IDECR is being written and DEV=0, or when SRST bit is asserted by Host or host system reset or D3-to-D0 transition of the IDE function. This bit is cleared by FW write of 0.
6	**Drive Ready (DRDY)** — R/W. When set, this bit indicates drive is ready for command.
5	**Drive Fault (DF)**— R/W. Indicates Error on the drive.
4	**Drive Seek Complete (DSC)**— R/W. Indicates Heads are positioned over the desired cylinder.
3	**Data Request (DRQ)**— R/W. Set when, the drive wants to exchange data with the Host using the data register.
2	**Corrected Data (CORR)**— R/W. When set, this bit indicates a correctable read error has occurred.
1	**Index (IDX)**— R/W. This bit is set once per rotation of the medium when the index mark passes under the read/write head.
0	**Error (ERR)**— R/W. When set, this bit indicates an error occurred in the process of executing the previous command. The Error Register of the selected device contains the error information.

17.3.2.21 IDESD1R—IDE Status Device 1 Register (IDER—D22:F2)

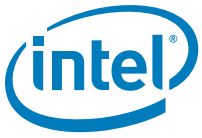
Address Offset:	07h	Attribute:	R/W
Default Value:	80h	Size:	8 bits

This register implements the status register of the slave device (DEV = 1). This register is read only by the Host. Host read of this register clears the slave device's interrupt.

When the HOST writes to the same address it writes to the command register.

The bits description is for ATA mode.

Bit	Description
7	**Busy (BSY)**— R/W. This bit is set by hardware when the IDECR is being written and DEV=0, or when SRST bit is asserted by the Host or host system reset or D3-to-D0 transition of the IDE function. This bit is cleared by FW write of 0.
6	**Drive Ready (DRDY)**— R/W. When set, indicates drive is ready for command.
5	**Drive Fault (DF)**— R/W. Indicates Error on the drive.
4	**Drive Seek Complete (DSC)** — R/W. Indicates Heads are positioned over the desired cylinder.
3	**Data Request (DRQ)** — R/W. Set when the drive wants to exchange data with the Host using the data register.
2	**Corrected Data (CORR)** — R/W**.** When set indicates a correctable read error has occurred.
1	**Index (IDX) —** R/W**.** This bit is set once per rotation of the medium when the index mark passes under the read/write head.
0	**Error (ERR)** — R/W**.** When set, this bit indicates an error occurred in the process of executing the previous command. The Error Register of the selected device contains the error information



17.3.2.22 IDECR—IDE Command Register (IDER—D22:F2)

Address Offset:	07h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register implements the Command register of the command block of the IDE function. This register can be written only by the Host.

When the HOST reads the same address it reads the Status register DEV0 if DEV=0 or Status Register DEV1 if DEV=1 (Drive/Head register bit [4]).

Bit	Description
7:0	**IDE Command Data (IDECD) — R/W.** Host sends the commands (read/ write, etc.) to the drive using this register.

17.3.3 IDER BAR1 Registers

Table 17-7. IDER BAR1 Register Address Map

Address Offset	Register Symbol	Register Name	Default Value	Attribute
2h	IDDCR	IDE Device Control Register	00h	RO, WO
2h	IDASR	IDE Alternate status Register	00h	RO

17.3.3.1 IDDCR—IDE Device Control Register (IDER—D22:F2)

Address Offset:	2h	Attribute:	WO
Default Value:	00h	Size:	8 bits

This register implements the Device Control register of the Control block of the IDE function. This register is Write only by the Host.

When the HOST reads to the same address it reads the Alternate Status register.

Bit	Description
7:3	Reserved
2	**Software reset (S_RST)** — WO. When this bit is set by the Host, it forces a reset to the device.
1	**Host interrupt Disable (nIEN)** — WO. When set, this bit disables hardware from sending interrupt to the Host.
0	Reserved

17.3.3.2 IDASR—IDE Alternate Status Register (IDER—D22:F2)

Address Offset:	2h	Attribute:	RO
Default Value:	00h	Size:	8 bits

This register implements the Alternate Status register of the Control block of the IDE function. This register is a mirror register to the status register in the command block. Reading this register by the HOST does not clear the IDE interrupt of the DEV selected device

Host read of this register when DEV=0 (Master), Host gets the mirrored data of IDESD0R register.

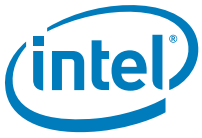
Host read of this register when DEV=1 (Slave), host gets the mirrored data of IDESD1R register.

Bit	Description
7:0	**IDE Alternate Status Register (IDEASR)**— RO. This field mirrors the value of the DEV0/ DEV1 status register, depending on the state of the DEV bit on Host reads.

17.3.4 IDER BAR4 Registers

Table 17-8. IDER BAR4 Register Address Map

Address Offset	Register Symbol	Register Name	Default Value	Attribute
0h	IDEPBMCR	IDE Primary Bus Master Command Register	00h	RO, R/W
1h	IDEPBMDS0R	IDE Primary Bus Master Device Specific 0 Register	00h	R/W
2h	IDEPBMSR	IDE Primary Bus Master Status Register	80h	RO, R/W
3h	IDEPBMDS1R	IDE Primary Bus Master Device Specific 1 Register	00h	R/W
4h	IDEPBMDTPR0	IDE Primary Bus Master Descriptor Table Pointer Register Byte 0	00h	R/W
5h	IDEPBMDTPR1	IDE Primary Bus Master Descriptor Table Pointer Register Byte 1	00h	R/W
6h	IDEPBMDTPR2	IDE Primary Bus Master Descriptor Table Pointer Register Byte 2	00h	R/W
7h	IDEPBMDTPR3	IDE Primary Bus Master Descriptor Table Pointer Register Byte 3	00h	R/W
8h	IDESBMCR	IDE Secondary Bus Master Command Register	00h	RO, R/W
9h	IDESBMDS0R	IDE Secondary Bus Master Device Specific 0 Register	00h	R/W
Ah	IDESBMSR	IDE Secondary Bus Master Status Register	00h	R/W, RO
Bh	IDESBMDS1R	IDE Secondary Bus Master Device Specific 1 Register	00h	R/W
Ch	IDESBMDTPR0	IDE Secondary Bus Master Descriptor Table Pointer Register Byte 0	00h	R/W
Dh	IDESBMDTPR1	IDE Secondary Bus Master Descriptor Table Pointer Register Byte 1	00h	R/W
Eh	IDESBMDTPR2	IDE Secondary Bus Master Descriptor Table Pointer Register Byte 2	00h	R/W
Fh	IDESBMDTPR3	IDE Secondary Bus Master Descriptor Table Pointer Register Byte 3	00h	R/W



17.3.4.1 IDEPBMCR—IDE Primary Bus Master Command Register (IDER—D22:F2)

Address Offset:	00h	Attribute:	RO, R/W
Default Value:	00h	Size:	8 bits

This register implements the bus master command register of the primary channel. This register is programmed by the Host.

Bit	Description
7:4	Reserved
3	**Read Write Command (RWC)** — R/W. This bit sets the direction of bus master transfer. 0 = Reads are performed from system memory 1 = Writes are performed to System Memory. This bit should not be changed when the bus master function is active.
2:1	Reserved
0	**Start/Stop Bus Master (SSBM)** — R/W**.** This bit gates the bus master operation of IDE function when 0. Writing 1 enables the bus master operation. Bus master operation can be halted by writing a 0 to this bit. Operation cannot be stopped and resumed. This bit is cleared after data transfer is complete as indicated by either the BMIA bit or the INT bit of the Bus Master status register is set or both are set.

17.3.4.2 IDEPBMDS0R—IDE Primary Bus Master Device Specific 0 Register (IDER—D22:F2)

Address Offset:	01h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

Bit	Description
7:0	**Device Specific Data0 (DSD0)** — R/W**.** Device Specific

17.3.4.3 IDEPBMSR—IDE Primary Bus Master Status Register (IDER—D22:F2)

Address Offset:	02h	Attribute:	RO, R/W
Default Value:	80h	Size:	8 bits

Bit	Description
7	**Simplex Only (SO)** — RO. Value indicates whether both Bus Master Channels can be operated at the same time or not. 0 = Both can be operated independently 1 = Only one can be operated at a time.
6	**Drive 1 DMA Capable (D1DC)** — R/W**.** This bit is read/write by the host (not write 1 clear).
5	**Drive 0 DMA Capable (D0DC)** — R/W**.** This bit is read/write by the host (not write 1 clear).
4:3	Reserved
2	**Interrupt (INT)** — R/W**.** This bit is set by the hardware when it detects a positive transition in the interrupt logic (refer to IDE host interrupt generation diagram).The hardware will clear this bit when the Host SW writes 1 to it.
1	**Error (ER)** — R/W**.** Bit is typically set by FW. Hardware will clear this bit when the Host SW writes 1 to it.
0	**Bus Master IDE Active (BMIA)** — RO. This bit is set by hardware when SSBM register is set to 1 by the Host. When the bus master operation ends (for the whole command) this bit is cleared by firmware. This bit is not cleared when the HOST writes 1 to it.

17.3.4.4 IDEPBMDS1R—IDE Primary Bus Master Device Specific 1 Register (IDER—D22:F2)

Address Offset: 03h Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Device Specific Data1 (DSD1)** — R/W. Device Specific Data.

17.3.4.5 IDEPBMDTPR0—IDE Primary Bus Master Descriptor Table Pointer Byte 0 Register (IDER—D22:F2)

Address Offset: 04h Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Descriptor Table Pointer Byte 0 (DTPB0)** — R/W. This register implements the Byte 0 (1 of 4 bytes) of the descriptor table Pointer (four I/O byte addresses) for bus master operation of the primary channel. This register is read/write by the HOST interface.

17.3.4.6 IDEPBMDTPR1—IDE Primary Bus Master Descriptor Table Pointer Byte 1 Register (IDER—D22:F2)

Address Offset: 05h Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Descriptor Table Pointer Byte 1 (DTPB1)** — R/W. This register implements the Byte 1 (of four bytes) of the descriptor table Pointer (four I/O byte addresses) for bus master operation of the primary channel. This register is programmed by the Host.

17.3.4.7 IDEPBMDTPR2—IDE Primary Bus Master Descriptor Table Pointer Byte 2 Register (IDER—D22:F2)

Address Offset: 06h Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Descriptor Table Pointer Byte 2 (DTPB2)** — R/W. This register implements the Byte 2 (of four bytes) of the descriptor table Pointer (four I/O byte addresses) for bus master operation of the primary channel. This register is programmed by the Host.

17.3.4.8 IDEPBMDTPR3—IDE Primary Bus Master Descriptor Table Pointer Byte 3 Register (IDER—D22:F2)

Address Offset: 07h Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Descriptor Table Pointer Byte 3 (DTPB3)** — R/W. This register implements the Byte 3 (of four bytes) of the descriptor table Pointer (four I/O byte addresses) for bus master operation of the primary channel. This register is programmed by the Host.

17.3.4.9 IDESBMCR—IDE Secondary Bus Master Command Register (IDER—D22:F2)

Address Offset: 08h Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:4	Reserved
3	**Read Write Command (RWC)** — R/W. This bit sets the direction of bus master transfer. When 0, Reads are performed from system memory; when 1, writes are performed to System Memory. This bit should not be changed when the bus master function is active.
2:1	Reserved
0	**Start/Stop Bus Master (SSBM)** — R/W. This bit gates the bus master operation of IDE function when zero. Writing 1 enables the bus master operation. Bus master operation can be halted by writing a 0 to this bit. Operation cannot be stopped and resumed. This bit is cleared after data transfer is complete as indicated by either the BMIA bit or the INT bit of the Bus Master status register is set or both are set.

17.3.4.10 IDESBMDS0R—IDE Secondary Bus Master Device Specific 0 Register (IDER—D22:F2)

Address Offset: 09h Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Device Specific Data0 (DSD0)** — R/W. This register implements the bus master Device Specific 1 register of the secondary channel. This register is programmed by the Host.

17.3.4.11 IDESBMSR—IDE Secondary Bus Master Status Register (IDER—D22:F2)

Address Offset: 0Ah Attribute: R/W, RO
Default Value: 80h Size: 8 bits

Bit	Description
7	**Simplex Only (SO)** — R/W. This bit indicates whether both Bus Master Channels can be operated at the same time or not. 0 = Both can be operated independently 1 = Only one can be operated at a time.
6	**Drive 1 DMA Capable (D1DC)** — R/W. This bit is read/write by the host.
5	**Drive 0 DMA Capable (D0DC)** — R/W. This bit is read/write by the host.
4:0	Reserved

17.3.4.12 IDESBMDS1R—IDE Secondary Bus Master Device Specific 1 Register (IDER—D22:F2)

Address Offset: 0Bh Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Device Specific Data1 (DSD1)** — R/W. This register implements the bus master Device Specific 1 register of the secondary channel. This register is programmed by the Host for device specific data if any.

17.3.4.13 IDESBMDTPR0—IDE Secondary Bus Master Descriptor Table Pointer Byte 0 Register (IDER—D22:F2)

Address Offset: 0Ch Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Descriptor Table Pointer Byte 0 (DTPB0)** — R/W. This register implements the Byte 0 (1 of 4 bytes) of the descriptor table Pointer (four I/O byte addresses) for bus master operation of the secondary channel. This register is read/write by the HOST interface.

17.3.4.14 IDESBMDTPR1—IDE Secondary Bus Master Descriptor Table Pointer Byte 1 Register (IDER—D22:F2)

Address Offset: 0Dh Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Descriptor Table Pointer Byte 1 (DTPB1)** — R/W. This register implements the Byte 1 (of four bytes) of the descriptor table Pointer (four I/O byte addresses) for bus master operation of the secondary channel. This register is programmed by the Host.

17.3.4.15 IDESBMDTPR2—IDE Secondary Bus Master Descriptor Table Pointer Byte 2 Register (IDER—D22:F2)

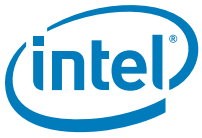
Address Offset: 0Eh Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Descriptor Table Pointer Byte 2 (DTPB2)** — R/W. This register implements the Byte 2 (of four bytes) of the descriptor table Pointer (four I/O byte addresses) for bus master operation of the secondary channel. This register is programmed by the Host.

17.3.4.16 IDESBMDTPR3—IDE Secondary Bus Master Descriptor Table Pointer Byte 3 Register (IDER—D22:F2)

Address Offset: 0Fh Attribute: R/W
Default Value: 00h Size: 8 bits

Bit	Description
7:0	**Descriptor Table Pointer Byte 3 (DTPB3)** — R/W. This register implements the Byte 3 (of four bytes) of the descriptor table Pointer (four I/O byte addresses) for bus master operation of the secondary channel. This register is programmed by the Host.



17.4 Serial Port for Remote Keyboard and Text (KT) Redirection (KT — D22:F3)

17.4.1 PCI Configuration Registers (KT — D22:F3)

Table 17-9. Serial Port for Remote Keyboard and Text (KT) Redirection Register Address Map

Address Offset	Register Symbol	Register Name	Default Value	Attribute
00h–01h	VID	Vendor Identification	8086h	RO
02h–03h	DID	Device Identification	See Register description	RO
04h–05h	CMD	Command Register	0000h	RO, R/W
06h–07h	STS	Device Status	00B0h	RO
08h	RID	Revision ID	See Register description	RO
09h–0Bh	CC	Class Codes	070002h	RO
0Ch	CLS	Cache Line Size	00h	RO
10h–13h	KTIBA	KT IO Block Base Address	00000001h	RO, R/W
14h–17h	KTMBA	KT Memory Block Base Address	00000000h	RO, R/W
2Ch–2Dh	SVID	Subsystem Vendor ID	0000h	R/WO
2Eh–2Fh	SID	Subsystem ID	8086h	R/WO
34h	CAP	Capabilities Pointer	C8h	RO
3Ch–3Dh	INTR	Interrupt Information	0200h	R/W, RO
C8h–C9h	PID	PCI Power Management Capability ID	D001h	RO
CAh–CBh	PC	PCI Power Management Capabilities	0023h	RO
D0h–D1h	MID	Message Signaled Interrupt Capability ID	0005h	RO
D2h–D3h	MC	Message Signaled Interrupt Message Control	0080h	RO, R/W
D4h–D7h	MA	Message Signaled Interrupt Message Address	00000000h	RO, R/W
D8h–DBh	MAU	Message Signaled Interrupt Message Upper Address	00000000h	RO, R/W
DCh–DDh	MD	Message Signaled Interrupt Message Data	0000h	R/W

17.4.1.1 VID—Vendor Identification Register (KT—D22:F3)

Address Offset: 00–01h
Default Value: 8086h
Attribute: RO
Size: 16 bits

Bit	Description
15:0	**Vendor ID (VID)** — RO. This is a 16-bit value assigned by Intel.

17.4.1.2 DID—Device Identification Register (KT—D22:F3)

Address Offset: 02–03h
Default Value: See bit description
Attribute: RO
Size: 16 bits

Bit	Description
15:0	**Device ID (DID)** — RO. This is a 16-bit value assigned to the Intel® Xeon® Processor D-1500 Product Family KT controller. See the *Specification Update* for the value of the DID Register.

17.4.1.3 CMD—Command Register (KT—D22:F3)

Address Offset: 04–05h Attribute: RO, R/W
Default Value: 0000h Size: 16 bits

Bit	Description
15:11	Reserved
10	**Interrupt Disable (ID)**— R/W. This bit disables pin-based INTx# interrupts. This bit has no effect on MSI operation. 1 = Internal INTx# messages will not be generated. 0 = Internal INTx# messages are generated if there is an interrupt **and** MSI is not enabled.
9:3	Reserved
2	**Bus Master Enable (BME)**— R/W. This bit controls the KT function's ability to act as a master for data transfers. This bit does not impact the generation of completions for split transaction commands. For KT, the only bus mastering activity is MSI generation.
1	**Memory Space Enable (MSE)**— R/W. This bit controls Access to the PT function's target memory space.
0	**I/O Space enable (IOSE)**— R/W. This bit controls access to the PT function's target I/O space.

17.4.1.4 STS—Device Status Register (KT—D22:F3)

Address Offset: 06–07h Attribute: RO
Default Value: 00B0h Size: 16 bits

Bit	Description
15:11	Reserved
10:9	**DEVSEL# Timing Status (DEVT)**— RO. This field controls the device select time for the PT function's PCI interface.
8:5	Reserved
4	**Capabilities List (CL)**— RO. This bit indicates that there is a capabilities pointer implemented in the device.
3	**Interrupt Status (IS)**— RO. This bit reflects the state of the interrupt in the function. Setting of the Interrupt Disable bit to 1 has no affect on this bit. Only when this bit is a 1 and ID bit is 0 is the INTB interrupt asserted to the Host.
2:0	Reserved

17.4.1.5 RID—Revision ID Register (KT—D22:F3)

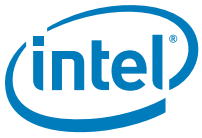
Address Offset: 08h Attribute: RO
Default Value: See bit description Size: 8 bits

Bit	Description
7:0	**Revision ID** — RO. See the *Specification Update* for the value of the RID Register.

17.4.1.6 CC—Class Codes Register (KT—D22:F3)

Address Offset: 09–0Bh Attribute: RO
Default Value: 070002h Size: 24 bits

Bit	Description
23:16	**Base Class Code (BCC)**—RO This field indicates the base class code of the KT host controller device.
15:8	**Sub Class Code (SCC)**—RO This field indicates the sub class code of the KT host controller device.
7:0	**Programming Interface (PI)**—RO This field indicates the programming interface of the KT host controller device.



17.4.1.7 CLS—Cache Line Size Register (KT—D22:F3)

Address Offset: 0Ch Attribute: RO
Default Value: 00h Size: 8 bits

This register defines the system cache line size in DWORD increments. Mandatory for master which use the Memory-Write and Invalidate command.

Bit	Description
7:0	**Cache Line Size (CLS)**— RO. All writes to system memory are Memory Writes.

17.4.1.8 KTIBA—KT IO Block Base Address Register (KT—D22:F3)

Address Offset: 10–13h Attribute: RO, R/W
Default Value: 00000001h Size: 32 bits

Bit	Description
31:16	Reserved
15:3	**Base Address (BAR)**— R/W. This field provides the base address of the I/O space (8 consecutive I/O locations).
2:1	Reserved
0	**Resource Type Indicator (RTE)**— RO. This bit indicates a request for I/O space

17.4.1.9 KTMBA—KT Memory Block Base Address Register (KT—D22:F3)

Address Offset: 14–17h Attribute: RO, R/W
Default Value: 00000000h Size: 32 bits

Bit	Description
31:12	**Base Address (BAR)**— R/W. This field provides the base address for Memory Mapped I,O BAR. Bits 31:12 correspond to address signals 31:12.
11:4	Reserved
3	**Prefetchable (PF)**— RO. This bit indicates that this range is not pre-fetchable.
2:1	**Type (TP)**— RO. This field indicates that this range can be mapped anywhere in 32-bit address space.
0	**Resource Type Indicator (RTE)**— RO. This bit indicates a request for register memory space.

17.4.1.10 SVID—Subsystem Vendor ID Register (KT—D22:F3)

Address Offset: 2Ch–2Dh Attribute: R/WO
Default Value: 0000h Size: 16 bits

Bit	Description
15:0	**Subsystem Vendor ID (SSVID)** — R/WO. Indicates the sub-system vendor identifier. This field should be programmed by BIOS during boot-up. Once written, this register becomes Read Only. This field can only be cleared by PLTRST#. ***Note:*** Register must be written as a DWord write with SID register.

17.4.1.11 SID—Subsystem ID Register (KT—D22:F3)

Address Offset: 2Eh–2Fh Attribute: R/WO
Default Value: 8086h Size: 16 bits

Bit	Description
15:0	**Subsystem ID (SSID)** — R/WO. Indicates the sub-system identifier. This field should be programmed by BIOS during boot-up. Once written, this register becomes Read Only. This field can only be cleared by PLTRST#. ***Note:*** Register must be written as a DWord write with SVID register.

17.4.1.12 CAP—Capabilities Pointer Register (KT—D22:F3)

Address Offset: 34h Attribute: RO
Default Value: C8h Size: 8 bits

This optional register is used to point to a linked list of new capabilities implemented by the device.

Bit	Description
7:0	**Capability Pointer (CP)**— RO. This field indicates that the first capability pointer is offset C8h (the power management capability).

17.4.1.13 INTR—Interrupt Information Register (KT—D22:F3)

Address Offset: 3C–3Dh Attribute: R/W, RO
Default Value: 0200h Size: 16 bits

Bit	Description
15:8	**Interrupt Pin (IPIN)**— RO. A value of 1h/2h/3h/4h indicates that this function implements legacy interrupt on INTA/INTB/INTC/INTD, respectively **FunctionValueINTx** (3 KT/Serial Port)02hINTB
7:0	**Interrupt Line (ILINE)**— R/W. The value written in this register tells which input of the system interrupt controller, the device's interrupt pin is connected to. This value is used by the OS and the device driver, and has no affect on the hardware.

17.4.1.14 PID—PCI Power Management Capability ID Register (KT—D22:F3)

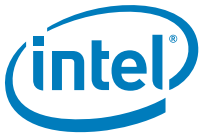
Address Offset: C8–C9h Attribute: RO
Default Value: D001h Size: 16 bits

Bit	Description
15:8	**Next Capability (NEXT)**— RO. A value of D0h points to the MSI capability.
7:0	**Cap ID (CID)**— RO. This field indicates that this pointer is a PCI power management.

17.4.1.15 PC—PCI Power Management Capabilities ID Register (KT—D22:F3)

Address Offset: CA–CBh Attribute: RO
Default Value: 0023h Size: 16 bits

Bit	Description
15:11	**PME Support (PME)**— RO.This field indicates no PME# in the PT function.
10:6	Reserved
5	**Device Specific Initialization (DSI)**— RO. This bit indicates that no device-specific initialization is required.
4	Reserved
3	**PME Clock (PMEC)**— RO. This bit indicates that PCI clock is not required to generate PME#
2:0	**Version (VS)**— RO. This field indicates support for the *PCI Power Management Specification, Revision 1.2*.



17.4.1.16 MID—Message Signaled Interrupt Capability ID Register (KT—D22:F3)

Address Offset:	D0–D1h	Attribute:	RO
Default Value:	0005h	Size:	16 bits

Message Signaled Interrupt is a feature that allows the device/function to generate an interrupt to the host by performing a DWORD memory write to a system specified address with system specified data. This register is used to identify and configure an MSI capable device.

Bit	Description
15:8	**Next Pointer (NEXT)**— RO. This value indicates this is the last item in the list.
7:0	**Capability ID (CID)**— RO. This field value of Capabilities ID indicates device is capable of generating MSI.

17.4.1.17 MC—Message Signaled Interrupt Message Control Register (KT—D22:F3)

Address Offset:	D2–D3h	Attribute:	RO, R/W
Default Value:	0080h	Size:	16 bits

Bit	Description
15:8	Reserved
7	**64-Bit Address Capable (C64)**— RO. Capable of generating 64-bit and 32-bit messages.
6:4	**Multiple Message Enable (MME)**— R/W.These bits are R/W for software compatibility, but only one message is ever sent by the PT function.
3:1	**Multiple Message Capable (MMC)**— RO. Only one message is required.
0	**MSI Enable (MSIE)**— R/W. If set, MSI is enabled and traditional interrupt pins are not used to generate interrupts.

17.4.1.18 MA—Message Signaled Interrupt Message Address Register (KT—D22:F3)

Address Offset:	D4–D7h	Attribute:	RO, R/W
Default Value:	00000000h	Size:	32 bits

This register specifies the DWORD aligned address programmed by system software for sending MSI.

Bit	Description
31:2	**Address (ADDR)**— R/W. Lower 32 bits of the system specified message address, always DWord aligned.
1:0	Reserved

17.4.1.19 MAU—Message Signaled Interrupt Message Upper Address Register (KT—D22:F3)

Address Offset: D8–DBh
Default Value: 00000000h
Attribute: RO, R/W
Size: 32 bits

Bit	Description
31:4	Reserved
3:0	**Address (ADDR)**— R/W. Upper 4 bits of the system specified message address.

17.4.1.20 MD—Message Signaled Interrupt Message Data Register (KT—D22:F3)

Address Offset: DC–DDh
Default Value: 0000h
Attribute: R/W
Size: 16 bits

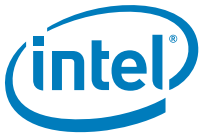
This 16-bit field is programmed by system software if MSI is enabled.

Bit	Description
15:0	**Data (DATA)**— R/W. This MSI data is driven onto the lower word of the data bus of the MSI memory write transaction.

17.4.2 KT IO/Memory Mapped Device Registers

Table 17-10. KT IO/Memory Mapped Device Register Address Map

Address Offset	Register Symbol	Register Name	Default Value	Attribute
0h	KTRxBR	KT Receive Buffer Register	00h	RO
0h	KTTHR	KT Transmit Holding Register	00h	WO
0h	KTDLLR	KT Divisor Latch LSB Register	00h	R/W
1h	KTIER	KT Interrupt Enable register	00h	R/W, RO
1h	KTDLMR	KT Divisor Latch MSB Register	00h	R/W
2h	KTIIR	KT Interrupt Identification register	01h	RO
2h	KTFCR	KT FIFO Control register	00h	WO
3h	KTLCR	KT Line Control register	03h	R/W
4h	KTMCR	KT Modem Control register	00h	RO, R/W
5h	KTLSR	KT Line Status register	00h	RO
6h	KTMSR	KT Modem Status register	00h	RO



17.4.2.1 KTRxBR—KT Receive Buffer Register (KT—D22:F3)

Address Offset:	00h	Attribute:	RO
Default Value:	00h	Size:	8 bits

This implements the KT Receiver Data register. Host access to this address, depends on the state of the DLAB bit (KTLCR[7]). It must be 0 to access the KTRxBR.

RxBR:

Host reads this register when FW provides it the receive data in non-FIFO mode. In FIFO mode, host reads to this register translate into a read from Intel ME memory (RBR FIFO).

Bit	Description
7:0	**Receiver Buffer Register (RBR)**— RO. Implements the Data register of the Serial Interface. If the Host does a read, it reads from the Receive Data Buffer.

17.4.2.2 KTTHR—KT Transmit Holding Register (KT—D22:F3)

Address Offset:	00h	Attribute:	RO
Default Value:	00h	Size:	8 bits

This implements the KT Transmit Data register. Host access to this address, depends on the state of the DLAB bit (KTLCR[7]). It must be 0 to access the KTTHR.

THR:

When host wants to transmit data in the non-FIFO mode, it writes to this register. In FIFO mode, writes by host to this address cause the data byte to be written by hardware to Intel ME memory (THR FIFO).

Bit	Description
7:0	**Transmit Holding Register (THR)**— WO. Implements the Transmit Data register of the Serial Interface. If the Host does a write, it writes to the Transmit Holding Register.

17.4.2.3 KTDLLR—KT Divisor Latch LSB Register (KT—D22:F3)

Address Offset:	00h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This register implements the KT DLL register. Host can Read/Write to this register only when the DLAB bit (KTLCR[7]) is 1. When this bit is 0, Host accesses the KTTHR or the KTRBR depending on Read or Write.

This is the standard Serial Port Divisor Latch register. This register is only for software compatibility and does not affect performance of the hardware.

Bit	Description
7:0	**Divisor Latch LSB (DLL)**— R/W. Implements the DLL register of the Serial Interface.

17.4.2.4 KTIER—KT Interrupt Enable Register (KT—D22:F3)

Address Offset:	01h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

This implements the KT Interrupt Enable register. Host access to this address, depends on the state of the DLAB bit (KTLCR[7]). It must be "0" to access this register. The bits enable specific events to interrupt the Host.

Bit	Description
7:4	Reserved
3	**MSR (IER2)**— R/W. When set, this bit enables bits in the Modem Status register to cause an interrupt to the host.
2	**LSR (IER1)**— R/W.When set, this bit enables bits in the Receiver Line Status Register to cause an Interrupt to the Host.
1	**THR (IER1)**— R/W. When set, this bit enables an interrupt to be sent to the Host when the transmit Holding register is empty.
0	**DR (IER0)**— R/W. When set, the Received Data Ready (or Receive FIFO Timeout) interrupts are enabled to be sent to Host.

17.4.2.5 KTDLMR—KT Divisor Latch MSB Register (KT—D22:F3)

Address Offset:	01h	Attribute:	R/W
Default Value:	00h	Size:	8 bits

Host can Read/Write to this register only when the DLAB bit (KTLCR[7]) is 1. When this bit is 0, Host accesses the KTIER.

This is the standard Serial interface's Divisor Latch register's MSB. This register is only for SW compatibility and does not affect performance of the hardware.

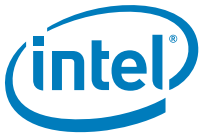
Bit	Description
7:0	**Divisor Latch MSB (DLM)**— R/W. Implements the Divisor Latch MSB register of the Serial Interface.

17.4.2.6 KTIIR—KT Interrupt Identification Register (KT—D22:F3)

Address Offset:	02h	Attribute:	RO
Default Value:	00h	Size:	8 bits

The KT IIR register prioritizes the interrupts from the function into 4 levels and records them in the IIR_STAT field of the register. When Host accesses the IIR, hardware freezes all interrupts and provides the priority to the Host. Hardware continues to monitor the interrupts but does not change its current indication until the Host read is over. Table in the Host Interrupt Generation section shows the contents.

Bit	Description
7	**FIFO Enable (FIEN1)**— RO. This bit is connected by hardware to bit 0 in the FCR register.
6	**FIFO Enable (FIEN0)**— RO. This bit is connected by hardware to bit 0 in the FCR register.
5:4	Reserved
3:1	**IIR STATUS (IIRSTS)**— RO. These bits are asserted by the hardware according to the source of the interrupt and the priority level.
0	**Interrupt Status (INTSTS)**— RO. 0 = Pending interrupt to Host 1 = No pending interrupt to Host



17.4.2.7 KTFCR—KT FIFO Control Register (KT—D22:F3)

Address Offset:	02h	Attribute:	WO
Default Value:	00h	Size:	8 bits

When Host writes to this address, it writes to the KTFCR. The FIFO control Register of the serial interface is used to enable the FIFOs, set the receiver FIFO trigger level and clear FIFOs under the direction of the Host.

When Host reads from this address, it reads the KTIIR.

Bit	Description
7:6	**Receiver Trigger Level (RTL)**— WO. Trigger level in bytes for the RCV FIFO. Once the trigger level number of bytes is reached, an interrupt is sent to the Host. 00 = 01 01 = 04 10 = 08 11 = 14
5:3	Reserved
2	**XMT FIFO Clear (XFIC)**— WO. When the Host writes one to this bit, the hardware will clear the XMT FIFO. This bit is self-cleared by hardware.
1	**RCV FIFO Clear (RFIC)**— WO. When the Host writes one to this bit, the hardware will clear the RCV FIFO. This bit is self-cleared by hardware.
0	**FIFO Enable (FIE)**— WO.When set, this bit indicates that the KT interface is working in FIFO node. When this bit value is changed the RCV and XMT FIFO are cleared by hardware.

17.4.2.8 KTLCR—KT Line Control Register (KT—D22:F3)

Address Offset:	03h	Attribute:	R/W
Default Value:	03h	Size:	8 bits

The line control register specifies the format of the asynchronous data communications exchange and sets the DLAB bit. Most bits in this register have no affect on hardware and are only used by the FW.

Bit	Description
7	**Divisor Latch Address Bit (DLAB)**— R/W. This bit is set when the Host wants to read/write the Divisor Latch LSB and MSB Registers. This bit is cleared when the Host wants to access the Receive Buffer Register or the Transmit Holding Register or the Interrupt Enable Register.
6	**Break Control (BC)**— R/W. This bit has no affect on hardware.
5:4	**Parity Bit Mode (PBM)**— R/W. This bit has no affect on hardware.
3	**Parity Enable (PE)**— R/W.This bit has no affect on hardware.
2	**Stop Bit Select (SBS)**— R/W. This bit has no affect on hardware.
1:0	**Word Select Byte (WSB)**— R/W. This bit has no affect on hardware.

17.4.2.9 KTMCR—KT Modem Control Register (KT—D22:F3)

Address Offset: 04h
Default Value: 00h
Attribute: R/W
Size: 8 bits

The Modem Control Register controls the interface with the modem. Since the FW emulates the modem, the Host communicates to the FW using this register. Register has impact on hardware when the Loopback mode is on.

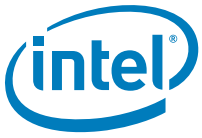
Bit	Description
7:5	Reserved
4	**Loop Back Mode (LBM)**— R/W. When set by the Host, this bit indicates that the serial port is in loop Back mode. This means that the data that is transmitted by the host should be received. Helps in debug of the interface.
3	**Output 2 (OUT2)**— R/W. This bit has no affect on hardware in normal mode. In loop back mode the value of this bit is written by hardware to the Modem Status Register bit 7.
2	**Output 1 (OUT1)**— R/W. This bit has no affect on hardware in normal mode. In loop back mode the value of this bit is written by hardware to Modem Status Register bit 6.
1	**Request to Send Out (RTSO)**— R/W. This bit has no affect on hardware in normal mode. In loopback mode, the value of this bit is written by hardware to Modem Status Register bit 4.
0	**Data Terminal Ready Out (DRTO)**— R/W. This bit has no affect on hardware in normal mode. In loopback mode, the value in this bit is written by hardware to Modem Status Register Bit 5.

17.4.2.10 KTLSR—KT Line Status Register (KT—D22:F3)

Address Offset: 05h
Default Value: 00h
Attribute: WO
Size: 8 bits

This register provides status information of the data transfer to the Host. Error indication, etc. are provided by the HW/FW to the host using this register.

Bit	Description
7	**RX FIFO Error (RXFER)**— RO. This bit is cleared in non FIFO mode. This bit is connected to BI bit in FIFO mode.
6	**Transmit Shift Register Empty (TEMT)**— RO. This bit is connected by HW to bit 5 (THRE) of this register.
5	**Transmit Holding Register Empty (THRE)**— RO. This bit is always set when the mode (FIFO/ Non-FIFO) is changed by the Host. This bit is active only when the THR operation is enabled by the FW. This bit has acts differently in the different modes: **Non FIFO**: This bit is cleared by hardware when the Host writes to the THR registers and set by hardware when the FW reads the THR register. **FIFO mode**: This bit is set by hardware when the THR FIFO is empty, and cleared by hardware when the THR FIFO is not empty. This bit is reset on Host system reset or D3->D0 transition.
4	**Break Interrupt (BI)**— RO. This bit is cleared by hardware when the LSR register is being read by the Host.
3:2	Reserved
1	**Overrun Error (OE):** This bit is cleared by hardware when the LSR register is being read by the Host. The FW typically sets this bit, but it is cleared by hardware when the host reads the LSR.
0	**Data Ready (DR)**— RO. **Non-FIFO Mode:** This bit is set when the FW writes to the RBR register and cleared by hardware when the RBR register is being Read by the Host. **FIFO Mode:** This bit is set by hardware when the RBR FIFO is not empty and cleared by hardware when the RBR FIFO is empty. This bit is reset on Host System Reset or D3->D0 transition.



17.4.2.11 KTMSR—KT Modem Status Register (KT—D22:F3)

Address Offset:	06h	Attribute:	RO
Default Value:	00h	Size:	8 bits

The functionality of the Modem is emulated by the FW. This register provides the status of the current state of the control lines from the modem.

Bit	Description
7	**Data Carrier Detect (DCD)** — RO. In Loop Back mode this bit is connected by hardware to the value of MCR bit 3.
6	**Ring Indicator (RI)** — RO. In Loop Back mode this bit is connected by hardware to the value of MCR bit 2.
5	**Data Set Ready (DSR)** — RO. In Loop Back mode this bit is connected by hardware to the value of MCR bit 0.
4	**Clear To Send (CTS)** — RO. In Loop Back mode this bit is connected by hardware to the value of MCR bit 1.
3	**Delta Data Carrier Detect (DDCD)** — RO. This bit is set when bit 7 is changed. This bit is cleared by hardware when the MSR register is being read by the HOST driver.
2	**Trailing Edge of Read Detector (TERI)** — RO. This bit is set when bit 6 is changed from 1 to 0. This bit is cleared by hardware when the MSR register is being read by the Host driver.
1	**Delta Data Set Ready (DDSR)** — RO. This bit is set when bit 5 is changed. This bit is cleared by hardware when the MSR register is being read by the Host driver.
0	**Delta Clear To Send (DCTS)** — RO. This bit is set when bit 4 is changed. This bit is cleared by hardware when the MSR register is being read by the Host driver.

§