

2nd Generation Intel® Core™ Processor Family Desktop, Intel® Pentium® Processor Family Desktop, and Intel® Celeron® Processor Family Desktop

Datasheet, Volume 1

Supporting Intel® Core™ i7, i5, and i3 Desktop Processor Series Supporting Intel® Pentium® Processor G800 and G600 Series Supporting Intel® Celeron® Processor G500 and G400 Series

This is Volume 1 of 2

June 2013

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY
APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the
absence or characteristics of any features or instructions marked "reserved" or "undefined." Int definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document 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.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. All products, platforms, dates, and figures specified are preliminary based on current expectations, and are subject to change

without notice. All dates specified are target dates, are provided for planning purposes only and are subject to change.

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group and specific software for some uses. For more information, see<http://www.intel.com/technology/security/>

Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain computer system software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

Intel[®] Active Management Technology requires the computer system to have an Intel(R) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see http://www.intel.com/technology/ platform-technology/intel-amt/

Hyper-Threading Technology requires a computer system with a processor supporting HT Technology and an HT Technologyenabled chipset, BIOS and operating system. Performance will vary depending on the specific hardware and software you use. For
more information including details on which processors support HT Technology, see htp://www.int

"Intel® Turbo Boost Technology requires a PC with a processor with Intel Turbo Boost Technology capability. Intel Turbo Boost Technology performance varies depending on hardware, software and overall system configuration. Check with your PC manufacturer on whether your system delivers Intel Turbo Boost Technology.For more information, see http://www.intel.com/ technology/turboboost."

Enhanced Intel[®] SpeedStep[®] Technology See the Processor Spec Finder or contact your Intel representative for more information.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See www.intel.com/products/processor_number for details.

64-bit computing on Intel architecture requires a computer system with a processor, chipset, BIOS, operating system, device
drivers and applications enabled for Intel® 64 architecture. Performance will vary depending on yo configurations. Consult with your system vendor for more information.

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

Intel, Intel Core, Celeron, Pentium, Speedstep, and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

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

Copyright © 2011–2013, Intel Corporation. All rights reserved.

Contents

Figures

Tables

§ §

1 Introduction

Figure 1-1. Desktop Platform System Block Diagram Example

1.1 Processor Feature Details

- Four or two execution cores
- A 32-KB instruction and 32-KB data first-level cache (L1) for each core
- A 256-KB shared instruction/data second-level cache (L2) for each core
- Up to 8-MB shared instruction/data third-level cache (L3), shared among all cores

1.1.1 Supported Technologies

- Intel[®] Virtualization Technology (Intel[®] VT) for Directed I/O (Intel[®] VT-d)
- Intel[®] Virtualization Technology (Intel[®] VT) for IA-32, Intel[®] 64 and Intel[®] Architecture (Intel® VT-x)
- Intel[®] Active Management Technology 7.0 (Intel[®] AMT 7.0)
- Intel[®] Trusted Execution Technology (Intel[®] TXT)
- Intel[®] Streaming SIMD Extensions 4.1 (Intel[®] SSE4.1)
- Intel[®] Streaming SIMD Extensions 4.2 (Intel[®] SSE4.2)
- Intel[®] Hyper-Threading Technology (Intel[®] HT Technology)
- Intel $^{\circledR}$ 64 Architecture
- Execute Disable Bit
- Intel[®] Turbo Boost Technology
- Intel $^{\circledR}$ Advanced Vector Extensions (Intel $^{\circledR}$ AVX)
- Intel[®] Advanced Encryption Standard New Instructions (Intel[®] AES-NI)
- PCLMULQDQ Instruction

1.2 Interfaces

1.2.1 System Memory Support

- Two channels of unbuffered DDR3 memory with a maximum of two UDIMMs or SO-DIMMs (for AIO) per channel
- Single-channel and dual-channel memory organization modes
- Data burst length of eight for all memory organization modes
- Memory DDR3 data transfer rates of 1066 MT/s and 1333 MT/s
- 64-bit wide channels
- DDR3 I/O Voltage of 1.5 V
- The type of memory supported by the processor is dependent on the PCH SKU in the target platform
	- Desktop PCH platforms support non-ECC un-buffered DIMMs only
	- All In One platforms (AIO) support SO-DIMMs
- Maximum memory bandwidth of 10.6 GB/s in single-channel mode or 21 GB/s in dual-channel mode assuming DDR3 1333 MT/s
- 1Gb, 2Gb, and 4Gb DDR3 DRAM technologies are supported
	- Using 4Gb device technologies, the largest memory capacity possible is 32 GB, assuming Dual Channel Mode with four x8 dual ranked unbuffered DIMM memory configuration.

- Up to 64 simultaneous open pages, 32 per channel (assuming 8 ranks of 8 bank devices)
- Command launch modes of 1n/2n
- On-Die Termination (ODT)
- Asynchronous ODT
- Intel[®] Fast Memory Access (Intel[®] FMA)
	- Just-in-Time Command Scheduling
	- Command Overlap
	- Out-of-Order Scheduling

1.2.2 PCI Express*

- PCI Express* port(s) are fully-compliant with the *PCI Express Base Specification, Revision 2.0*.
- Processor with desktop PCH supported configurations

Table 1-1. PCI Express* Supported Configurations in Desktop Products

- The port may negotiate down to narrower widths — Support for x16/x8/x4/x1 widths for a single PCI Express mode
- 2.5 GT/s and 5.0 GT/s PCI Express* frequencies are supported
- Gen1 Raw bit-rate on the data pins of 2.5 GT/s, resulting in a real bandwidth per pair of 250 MB/s given the 8b/10b encoding used to transmit data across this interface. This also does not account for packet overhead and link maintenance.
- Maximum theoretical bandwidth on the interface of 4 GB/s in each direction simultaneously, for an aggregate of 8 GB/s when x16 Gen 1
- Gen 2 Raw bit-rate on the data pins of 5.0 GT/s, resulting in a real bandwidth per pair of 500 MB/s given the 8b/10b encoding used to transmit data across this interface. This also does not account for packet overhead and link maintenance.
- Maximum theoretical bandwidth on the interface of 8 GB/s in each direction simultaneously, for an aggregate of 16 GB/s when x16 Gen 2
- Hierarchical PCI-compliant configuration mechanism for downstream devices
- Traditional PCI style traffic (asynchronous snooped, PCI ordering)
- PCI Express* extended configuration space. The first 256 bytes of configuration space aliases directly to the PCI Compatibility configuration space. The remaining portion of the fixed 4-KB block of memory-mapped space above that (starting at 100h) is known as extended configuration space.
- PCI Express* Enhanced Access Mechanism; accessing the device configuration space in a flat memory mapped fashion
- Automatic discovery, negotiation, and training of link out of reset
- Traditional AGP style traffic (asynchronous non-snooped, PCI-X Relaxed ordering)
- Peer segment destination posted write traffic (no peer-to-peer read traffic) in Virtual Channel 0
	- DMI -> PCI Express* Port 0

- 64-bit downstream address format, but the processor never generates an address above 64 GB (Bits 63:36 will always be zeros)
- 64-bit upstream address format, but the processor responds to upstream read transactions to addresses above 64 GB (addresses where any of Bits 63:36 are nonzero) with an Unsupported Request response. Upstream write transactions to addresses above 64 GB will be dropped.
- Re-issues Configuration cycles that have been previously completed with the Configuration Retry status
- PCI Express* reference clock is 100-MHz differential clock
- Power Management Event (PME) functions
- Dynamic width capability
- Message Signaled Interrupt (MSI and MSI-X) messages
- Polarity inversion

Note: The processor does not support PCI Express* Hot-Plug.

1.2.3 Direct Media Interface (DMI)

- DMI 2.0 support
- Four lanes in each direction
- 5 GT/s point-to-point DMI interface to PCH is supported
- Raw bit-rate on the data pins of 5.0 GB/s, resulting in a real bandwidth per pair of 500 MB/s given the 8b/10b encoding used to transmit data across this interface. Does not account for packet overhead and link maintenance.
- Maximum theoretical bandwidth on interface of 2 GB/s in each direction simultaneously, for an aggregate of 4 GB/s when DMI x4
- Shares 100-MHz PCI Express* reference clock
- 64-bit downstream address format, but the processor never generates an address above 64 GB (Bits 63:36 will always be zeros)
- 64-bit upstream address format, but the processor responds to upstream read transactions to addresses above 64 GB (addresses where any of Bits 63:36 are nonzero) with an Unsupported Request response. Upstream write transactions to addresses above 64 GB will be dropped.
- Supports the following traffic types to or from the PCH
	- DMI -> DRAM
	- DMI -> processor core (Virtual Legacy Wires (VLWs), Resetwarn, or MSIs only) — Processor core -> DMI
- APIC and MSI interrupt messaging support
	- Message Signaled Interrupt (MSI and MSI-X) messages
- Downstream SMI, SCI and SERR error indication
- Legacy support for ISA regime protocol (PHOLD/PHOLDA) required for parallel port DMA, floppy drive, and LPC bus masters
- DC coupling no capacitors between the processor and the PCH
- Polarity inversion
- PCH end-to-end lane reversal across the link
- Supports Half Swing "low-power/low-voltage"

1.2.4 Platform Environment Control Interface (PECI)

The PECI is a one-wire interface that provides a communication channel between a PECI client (the processor) and a PECI master. The processors support the PECI 3.0 Specification.

1.2.5 Processor Graphics

- The Processor Graphics contains a refresh of the sixth generation graphics core enabling substantial gains in performance and lower power consumption.
- Next Generation Intel Clear Video Technology HD support is a collection of video playback and enhancement features that improve the end user's viewing experience.
	- Encode/transcode HD content
	- Playback of high definition content including Blu-ray Disc*
	- Superior image quality with sharper, more colorful images
	- Playback of Blu-ray disc S3D content using HDMI (V.1.4 with 3D)
- DirectX* Video Acceleration (DXVA) support for accelerating video processing — Full AVC/VC1/MPEG2 HW Decode
- Advanced Scheduler 2.0, 1.0, XPDM support
- Windows* 7, XP, Windows Vista*, OSX, Linux OS Support
- DX10.1, DX10, DX9 support
- OGL 3.0 support
- Switchable graphics support on desktop AIO platforms with MxM solutions only

1.2.6 Intel® Flexible Display Interface (Intel® FDI)

- For SKUs with graphics, Intel FDI carries display traffic from the Processor Graphics in the processor to the legacy display connectors in the PCH
- Based on DisplayPort standard
- Two independent links one for each display pipe
- Four unidirectional downstream differential transmitter pairs
	- Scalable down to 3X, 2X, or 1X based on actual display bandwidth requirements
	- Fixed frequency 2.7 GT/s data rate
- Two sideband signals for Display synchronization — FDI_FSYNC and FDI_LSYNC (Frame and Line Synchronization)
- One Interrupt signal used for various interrupts from the PCH — FDI_INT signal shared by both Intel FDI Links
- PCH supports end-to-end lane reversal across both links
- Common 100-MHz reference clock

1.3 Power Management Support

1.3.1 Processor Core

- Full support of Advanced Configuration and Power Interface (ACPI) C-states as implemented by the following processor C-states
	- C0, C1, C1E, C3, C6
- Enhanced Intel SpeedStep[®] Technology

1.3.2 System

• S0, S3, S4, S5

1.3.3 Memory Controller

- Conditional self-refresh (Intel[®] Rapid Memory Power Management (Intel[®] RMPM))
- Dynamic power-down

1.3.4 PCI Express*

• L0s and L1 ASPM power management capability

1.3.5 Direct Media Interface (DMI)

• L0s and L1 ASPM power management capability

1.3.6 Processor Graphics Controller

- Intel[®] Rapid Memory Power Management (Intel[®] RMPM) CxSR
- Intel[®] Graphics Performance Modulation Technology (Intel[®] GPMT)
- Intel Smart 2D Display Technology (Intel S2DDT)
- Graphics Render C-State (RC6)

1.4 Thermal Management Support

- Digital Thermal Sensor
- Intel Adaptive Thermal Monitor
- THERMTRIP# and PROCHOT# support
- On-Demand Mode
- Memory Thermal Throttling
- External Thermal Sensor (TS-on-DIMM and TS-on-Board)
- Render Thermal Throttling
- Fan speed control with DTS

1.5 Package

- The processor socket type is noted as LGA 1155. The package is a 37.5 x 37.5 mm Flip Chip Land Grid Array (FCLGA 1155).
- *Note:* See the *2nd Generation Intel® Core™ Processor, Intel® Pentium® Processor, and Intel® Celeron® Processor, and LGA1155 Socket Thermal Mechanical Specifications and Design Guidelines* for complete details on package.

1.6 Terminology

Table 1-2. Terminology (Sheet 1 of 2)

Table 1-2. Terminology (Sheet 2 of 2)

1.7 Related Documents

Refer to [Table 1-3](#page-17-1) for additional information.

Table 1-3. Related Documents

§ §

2 Interfaces

This chapter describes the interfaces supported by the processor.

2.1 System Memory Interface

2.1.1 System Memory Technology Supported

The Integrated Memory Controller (IMC) supports DDR3 protocols with two independent, 64-bit wide channels each accessing one or two DIMMs. The type of memory supported by the processor is dependant on the PCH SKU in the target platform. Refer to [Chapter 1](#page-8-1) for supported memory configuration details.

It supports a maximum of two DDR3 DIMMs per-channel; thus, allowing up to four device ranks per-channel.

- DDR3 Data Transfer Rates
	- 1066 MT/s (PC3-8500), 1333 MT/s (PC3-10600)
- DDR3 SO-DIMM Modules
	- Raw Card A Dual Ranked x16 unbuffered non-ECC
	- Raw Card B Single Ranked x8 unbuffered non-ECC
	- Raw Card C Single Ranked x16 unbuffered non-ECC
	- Raw Card F Dual Ranked x8 (planar) unbuffered non-ECC
- Desktop PCH platform DDR3 DIMM Modules
	- Raw Card A Single Ranked x8 unbuffered non-ECC
	- Raw Card B Dual Ranked x8 unbuffered non-ECC
	- Raw Card C Single Ranked x16 unbuffered non-ECC
- Advanced Server/Workstation PCH platforms DDR3 DIMM Modules:
	- Raw Card A Single Ranked x8 unbuffered non-ECC
	- Raw Card B Dual Ranked x8 unbuffered non-ECC
	- Raw Card C Single Ranked x16 unbuffered non-ECC
	- Raw Card D Single Ranked x8 unbuffered ECC
	- Raw Card E Dual Ranked x8 unbuffered ECC
- Essential/Standard Server PCH platforms DDR3 DIMM Modules:
	- Raw Card D Single Ranked x8 unbuffered ECC
	- Raw Card E Dual Ranked x8 unbuffered ECC

DDR3 DRAM Device Technology: 1-Gb, 2-Gb, and 4 Gb DDR3 DRAM Device technologies and addressing are supported.

Table 2-1. Supported UDIMM Module Configurations

Note: DIMM module support is based on availability and is subject to change.

Table 2-2. Supported SO-DIMM Module Configurations (AIO Only)^{1,2}

Notes:
1. Sy
2. Int 1. System memory configurations are based on availability and are subject to change. 2. Interface does not support ULV/LV memory modules or ULV/LV DIMMs.

2.1.2 System Memory Timing Support

The IMC supports the following DDR3 Speed Bin, CAS Write Latency (CWL), and command signal mode timings on the main memory interface:

- t_{C1} = CAS Latency
- t_{RCD} = Activate Command to READ or WRITE Command delay
- t_{RP} = PRECHARGE Command Period
- CWL = CAS Write Latency
- Command Signal modes = 1n indicates a new command may be issued every clock and 2n indicates a new command may be issued every 2 clocks. Command launch mode programming depends on the transfer rate and memory configuration.

Table 2-3. DDR3 System Memory Timing Support

Notes:

^{11.} System memory timing support is based on availability and is subject to change.

2.1.3 System Memory Organization Modes

The IMC supports two memory organization modes—single-channel and dual-channel. Depending upon how the DIMM Modules are populated in each memory channel, a number of different configurations can exist.

2.1.3.1 Single-Channel Mode

In this mode, all memory cycles are directed to a single-channel. Single-channel mode is used when either Channel A or Channel B DIMM connectors are populated in any order, but not both.

2.1.3.2 Dual-Channel Mode – Intel® Flex Memory Technology Mode

The IMC supports Intel Flex Memory Technology Mode. Memory is divided into a symmetric and an asymmetric zone. The symmetric zone starts at the lowest address in each channel and is contiguous until the asymmetric zone begins or until the top address of the channel with the smaller capacity is reached. In this mode, the system runs with one zone of dual-channel mode and one zone of single-channel mode, simultaneously, across the whole memory array.

Note: Channels A and B can be mapped for physical channels 0 and 1 respectively or vice versa; however, channel A size must be greater or equal to channel B size.

Figure 2-1. Intel® Flex Memory Technology Operation

2.1.3.2.1 Dual-Channel Symmetric Mode

Dual-Channel Symmetric mode, also known as interleaved mode, provides maximum performance on real world applications. Addresses are ping-ponged between the channels after each cache line (64-byte boundary). If there are two requests, and the second request is to an address on the opposite channel from the first, that request can be sent before data from the first request has returned. If two consecutive cache lines are requested, both may be retrieved simultaneously since they are ensured to be on opposite channels. Use Dual-Channel Symmetric mode when both Channel A and Channel B DIMM connectors are populated in any order, with the total amount of memory in each channel being the same.

When both channels are populated with the same memory capacity and the boundary between the dual channel zone and the single channel zone is the top of memory, IMC operates completely in Dual-Channel Symmetric mode.

Note: The DRAM device technology and width may vary from one channel to the other.

2.1.4 Rules for Populating Memory Slots

In all modes, the frequency of system memory is the lowest frequency of all memory modules placed in the system, as determined through the SPD registers on the memory modules. The system memory controller supports one or two DIMM connectors per channel. The usage of DIMM modules with different latencies is allowed, but in that case, the worst latency (per channel) will be used. For dual-channel modes, both channels must have a DIMM connector populated and for single-channel mode, only a single-channel may have one or both DIMM connectors populated.

Note: In a 2 DIMM Per Channel (2DPC) daisy chain layout memory configuration, the furthest DIMM from the processor of any given channel must always be populated first.

2.1.5 Technology Enhancements of Intel® Fast Memory Access (Intel® FMA)

The following sections describe the Just-in-Time Scheduling, Command Overlap, and Out-of-Order Scheduling Intel FMA technology enhancements.

2.1.5.1 Just-in-Time Command Scheduling

The memory controller has an advanced command scheduler where all pending requests are examined simultaneously to determine the most efficient request to be issued next. The most efficient request is picked from all pending requests and issued to system memory Just-in-Time to make optimal use of Command Overlapping. Thus, instead of having all memory access requests go individually through an arbitration mechanism forcing requests to be executed one at a time, they can be started without interfering with the current request allowing for concurrent issuing of requests. This allows for optimized bandwidth and reduced latency while maintaining appropriate command spacing to meet system memory protocol.

2.1.5.2 Command Overlap

Command Overlap allows the insertion of the DRAM commands between the Activate, Precharge, and Read/Write commands normally used, as long as the inserted commands do not affect the currently executing command. Multiple commands can be issued in an overlapping manner, increasing the efficiency of system memory protocol.

2.1.5.3 Out-of-Order Scheduling

While leveraging the Just-in-Time Scheduling and Command Overlap enhancements, the IMC continuously monitors pending requests to system memory for the best use of bandwidth and reduction of latency. If there are multiple requests to the same open page, these requests would be launched in a back to back manner to make optimum use of the open memory page. This ability to reorder requests on the fly allows the IMC to further reduce latency and increase bandwidth efficiency.

2.1.6 Memory Type Range Registers (MTRRs) Enhancement

The processor has 2 additional MTRRs (total 10 MTRRs). These additional MTRRs are specially important in supporting larger system memory beyond 4 GB.

2.1.7 Data Scrambling

The memory controller incorporates a DDR3 Data Scrambling feature to minimize the impact of excessive di/dt on the platform DDR3 VRs due to successive 1s and 0s on the data bus. Past experience has demonstrated that traffic on the data bus is not random and can have energy concentrated at specific spectral harmonics creating high di/dt that is generally limited by data patterns that excite resonance between the package inductance and on-die capacitances. As a result, the memory controller uses a data scrambling feature to create pseudo-random patterns on the DDR3 data bus to reduce the impact of any excessive di/dt.

2.2 PCI Express* Interface

This section describes the PCI Express interface capabilities of the processor. See the *PCI Express Base Specification* for details of PCI Express.

The number of PCI Express controllers is dependent on the platform. Refer to [Chapter 1](#page-8-1) for details.

2.2.1 PCI Express* Architecture

Compatibility with the PCI addressing model is maintained to ensure that all existing applications and drivers operate unchanged.

The PCI Express configuration uses standard mechanisms as defined in the PCI Plug-and-Play specification. The initial recovered clock speed of 1.25 GHz results in 2.5 Gb/s/direction that provides a 250 MB/s communications channel in each direction (500 MB/s total). That is close to twice the data rate of classic PCI. The fact that 8b/10b encoding is used accounts for the 250 MB/s where quick calculations would imply 300 MB/s. The external graphics ports support Gen2 speed as well. At 5.0 GT/s, Gen 2 operation results in twice as much bandwidth per lane as compared to Gen 1 operation. When operating with two PCIe controllers, each controller can be operating at either 2.5 GT/s or 5.0 GT/s.

The PCI Express architecture is specified in three layers—Transaction Layer, Data Link Layer, and Physical Layer. The partitioning in the component is not necessarily along these same boundaries. Refer to [Figure 2-2](#page-23-2) for the PCI Express Layering Diagram.

Figure 2-2. PCI Express* Layering Diagram

PCI Express uses packets to communicate information between components. Packets are formed in the Transaction and Data Link Layers to carry the information from the transmitting component to the receiving component. As the transmitted packets flow through the other layers, they are extended with additional information necessary to

handle packets at those layers. At the receiving side, the reverse process occurs and packets get transformed from their Physical Layer representation to the Data Link Layer representation and finally (for Transaction Layer Packets) to the form that can be processed by the Transaction Layer of the receiving device.

Figure 2-3. Packet Flow through the Layers

2.2.1.1 Transaction Layer

The upper layer of the PCI Express architecture is the Transaction Layer. The Transaction Layer's primary responsibility is the assembly and disassembly of Transaction Layer Packets (TLPs). TLPs are used to communicate transactions, such as read and write, as well as certain types of events. The Transaction Layer also manages flow control of TLPs.

2.2.1.2 Data Link Layer

The middle layer in the PCI Express stack, the Data Link Layer, serves as an intermediate stage between the Transaction Layer and the Physical Layer. Responsibilities of Data Link Layer include link management, error detection, and error correction.

The transmission side of the Data Link Layer accepts TLPs assembled by the Transaction Layer, calculates and applies data protection code and TLP sequence number, and submits them to Physical Layer for transmission across the Link. The receiving Data Link Layer is responsible for checking the integrity of received TLPs and for submitting them to the Transaction Layer for further processing. On detection of TLP error(s), this layer is responsible for requesting retransmission of TLPs until information is correctly received, or the Link is determined to have failed. The Data Link Layer also generates and consumes packets that are used for Link management functions.

2.2.1.3 Physical Layer

The Physical Layer includes all circuitry for interface operation, including driver and input buffers, parallel-to-serial and serial-to-parallel conversion, PLL(s), and impedance matching circuitry. It also includes logical functions related to interface initialization and maintenance. The Physical Layer exchanges data with the Data Link Layer in an implementation-specific format, and is responsible for converting this to an appropriate serialized format and transmitting it across the PCI Express Link at a frequency and width compatible with the remote device.

2.2.2 PCI Express* Configuration Mechanism

The PCI Express (external graphics) link is mapped through a PCI-to-PCI bridge structure.

Figure 2-4. PCI Express* Related Register Structures in the Processor

PCI Express extends the configuration space to 4096 bytes per-device/function, as compared to 256 bytes allowed by the Conventional PCI Specification. PCI Express configuration space is divided into a PCI-compatible region (that consists of the first 256 bytes of a logical device's configuration space) and an extended PCI Express region (that consists of the remaining configuration space). The PCI-compatible region can be accessed using either the mechanisms defined in the PCI specification or using the enhanced PCI Express configuration access mechanism described in the PCI Express Enhanced Configuration Mechanism section.

The PCI Express Host Bridge is required to translate the memory-mapped PCI Express configuration space accesses from the host processor to PCI Express configuration cycles. To maintain compatibility with PCI configuration addressing mechanisms, it is recommended that system software access the enhanced configuration space using 32-bit operations (32-bit aligned) only. See the *PCI Express Base Specification* for details of both the PCI-compatible and PCI Express Enhanced configuration mechanisms and transaction rules.

2.2.3 PCI Express* Port

The PCI Express interface on the processor is a single, 16-lane (x16) port that can also be configured at narrower widths. The PCI Express port is compliant with the *PCI Express Base Specification, Revision 2.0.*

2.2.4 PCI Express* Lanes Connection

[Figure 2-5](#page-26-4) demonstrates the PCIe lanes mapping.

```
Figure 2-5. PCI Express* Typical Operation 16 lanes Mapping
```


2.3 Direct Media Interface (DMI)

Direct Media Interface (DMI) connects the processor and the PCH. Next generation DMI2 is supported.

Note: Only DMI x4 configuration is supported.

2.3.1 DMI Error Flow

DMI can only generate SERR in response to errors, never SCI, SMI, MSI, PCI INT, or GPE. Any DMI related SERR activity is associated with Device 0.

2.3.2 Processor / PCH Compatibility Assumptions

The processor is compatible with the Intel $^{\circledR}$ 6 Series Chipset PCH. The processor is not compatible with any previous PCH products.

2.3.3 DMI Link Down

The DMI link going down is a fatal, unrecoverable error. If the DMI data link goes to data link down, after the link was up, then the DMI link hangs the system by not allowing the link to retrain to prevent data corruption. This link behavior is controlled by the PCH.

Downstream transactions that had been successfully transmitted across the link prior to the link going down may be processed as normal. No completions from downstream, non-posted transactions are returned upstream over the DMI link after a link down event.

2.4 Processor Graphics Controller (GT)

New Graphics Engine Architecture includes 3D compute elements, Multi-format hardware-assisted decode/encode Pipeline, and Mid-Level Cache (MLC) for superior high definition playback, video quality, and improved 3D performance and Media.

Display Engine in the Uncore handles delivering the pixels to the screen. GSA (Graphics in System Agent) is the primary Channel interface for display memory accesses and "PCI-like" traffic in and out.

Figure 2-6. Processor Graphics Controller Unit Block Diagram

2.4.1 3D and Video Engines for Graphics Processing

The 3D graphics pipeline architecture simultaneously operates on different primitives or on different portions of the same primitive. All the cores are fully programmable, increasing the versatility of the 3D Engine. The Gen 6.0 3D engine provides the following performance and power-management enhancements:

- Up to 12 Execution units (EUs)
- Hierarchal-Z
- Video quality enhancements

2.4.1.1 3D Engine Execution Units

- Supports up to 12 EUs. The EUs perform 128-bit wide execution per clock.
- Support SIMD8 instructions for vertex processing and SIMD16 instructions for pixel processing.

2.4.1.2 3D Pipeline

2.4.1.2.1 Vertex Fetch (VF) Stage

The VF stage executes 3DPRIMITIVE commands. Some enhancements have been included to better support legacy D3D APIs as well as SGI OpenGL*.

2.4.1.2.2 Vertex Shader (VS) Stage

The VS stage performs shading of vertices output by the VF function. The VS unit produces an output vertex reference for every input vertex reference received from the VF unit, in the order received.

2.4.1.2.3 Geometry Shader (GS) Stage

The GS stage receives inputs from the VS stage. Compiled application-provided GS programs, specifying an algorithm to convert the vertices of an input object into some output primitives. For example, a GS shader may convert lines of a line strip into polygons representing a corresponding segment of a blade of grass centered on the line. Or it could use adjacency information to detect silhouette edges of triangles and output polygons extruding out from the edges.

2.4.1.2.4 Clip Stage

The Clip stage performs general processing on incoming 3D objects. However, it also includes specialized logic to perform a Clip Test function on incoming objects. The Clip Test optimizes generalized 3D Clipping. The Clip unit examines the position of incoming vertices, and accepts/rejects 3D objects based on its Clip algorithm.

2.4.1.2.5 Strips and Fans (SF) Stage

The SF stage performs setup operations required to rasterize 3D objects. The outputs from the SF stage to the Windower stage contain implementation-specific information required for the rasterization of objects and also supports clipping of primitives to some extent.

2.4.1.2.6 Windower/IZ (WIZ) Stage

The WIZ unit performs an early depth test, which removes failing pixels and eliminates unnecessary processing overhead.

The Windower uses the parameters provided by the SF unit in the object-specific rasterization algorithms. The WIZ unit rasterizes objects into the corresponding set of pixels. The Windower is also capable of performing dithering, whereby the illusion of a higher resolution when using low-bpp channels in color buffers is possible. Color dithering diffuses the sharp color bands seen on smooth-shaded objects.

2.4.1.3 Video Engine

The Video Engine handles the non-3D (media/video) applications. It includes support for VLD and MPEG2 decode in hardware.

2.4.1.4 2D Engine

The 2D Engine contains BLT (Block Level Transfer) functionality and an extensive set of 2D instructions. To take advantage of the 3D during engine's functionality, some BLT functions make use of the 3D renderer.

2.4.1.4.1 Processor Graphics VGA Registers

The 2D registers consists of original VGA registers and others to support graphics modes that have color depths, resolutions, and hardware acceleration features that go beyond the original VGA standard.

2.4.1.4.2 Logical 128-Bit Fixed BLT and 256 Fill Engine

This BLT engine accelerates the GUI of Microsoft Windows* operating systems. The 128-bit BLT engine provides hardware acceleration of block transfers of pixel data for many common Windows operations. The BLT engine can be used for the following:

- Move rectangular blocks of data between memory locations
- Data alignment
- To perform logical operations (raster ops)

The rectangular block of data does not change, as it is transferred between memory locations. The allowable memory transfers are between: cacheable system memory and frame buffer memory, frame buffer memory and frame buffer memory, and within system memory. Data to be transferred can consist of regions of memory, patterns, or solid color fills. A pattern is always 8×8 pixels wide and may be 8 , 16, or 32 bits per pixel.

The BLT engine expands monochrome data into a color depth of 8, 16, or 32 bits. BLTs can be either opaque or transparent. Opaque transfers move the data specified to the destination. Transparent transfers compare destination color to source color and write according to the mode of transparency selected.

Data is horizontally and vertically aligned at the destination. If the destination for the BLT overlaps with the source memory location, the BLT engine specifies which area in memory to begin the BLT transfer. Hardware is included for all 256 raster operations (source, pattern, and destination) defined by Microsoft, including transparent BLT.

The BLT engine has instructions to invoke BLT and stretch BLT operations, permitting software to set up instruction buffers and use batch processing. The BLT engine can perform hardware clipping during BLTs.

2.4.2 Processor Graphics Display

The Processor Graphics controller display pipe can be broken down into three components:

- Display Planes
- Display Pipes
- DisplayPort and Intel FDI

Figure 2-7. Processor Display Block Diagram

2.4.2.1 Display Planes

A display plane is a single displayed surface in memory and contains one image (desktop, cursor, overlay). It is the portion of the display hardware logic that defines the format and location of a rectangular region of memory that can be displayed on display output device and delivers that data to a display pipe. This is clocked by the Core Display Clock.

2.4.2.1.1 Planes A and B

Planes A and B are the main display planes and are associated with Pipes A and B respectively. The two display pipes are independent, allowing for support of two independent display streams. They are both double-buffered, which minimizes latency and improves visual quality.

2.4.2.1.2 Sprite A and B

Sprite A and Sprite B are planes optimized for video decode, and are associated with Planes A and B respectively. Sprite A and B are also double-buffered.

2.4.2.1.3 Cursors A and B

Cursors A and B are small, fixed-sized planes dedicated for mouse cursor acceleration, and are associated with Planes A and B respectively. These planes support resolutions up to 256 x 256 each.

2.4.2.1.4 Video Graphics Array (VGA)

VGA is used for boot, safe mode, legacy games, etc. It can be changed by an application without OS/driver notification, due to legacy requirements.

2.4.2.2 Display Pipes

The display pipe blends and synchronizes pixel data received from one or more display planes and adds the timing of the display output device upon which the image is displayed. This is clocked by the Display Reference clock inputs.

The display pipes A and B operate independently of each other at the rate of 1 pixel per clock. They can attach to any of the display ports. Each pipe sends display data to the PCH over the Intel Flexible Display Interface (Intel FDI).

2.4.2.3 Display Ports

The display ports consist of output logic and pins that transmit the display data to the associated encoding logic and send the data to the display device (that is, LVDS, HDMI*, DVI, SDVO, and so on). All display interfaces connecting external displays are now repartitioned and driven from the PCH.

2.4.3 Intel® Flexible Display Interface (Intel® FDI)

The Intel Flexible Display Interface (Intel® FDI) is a proprietary link for carrying display traffic from the Processor Graphics controller to the PCH display I/Os. Intel[®] FDI supports two independent channels—one for pipe A and one for pipe B.

- Each channel has four transmit (Tx) differential pairs used for transporting pixel and framing data from the display engine.
- Each channel has one single-ended LineSync and one FrameSync input (1-V CMOS signaling).
- One display interrupt line input (1-V CMOS signaling).
- Intel[®] FDI may dynamically scalable down to 2X or 1X based on actual display bandwidth requirements.
- Common 100-MHz reference clock.
- Each channel transports at a rate of 2.7 Gbps.
- PCH supports end-to-end lane reversal across both channels (no reversal support required in the processor).

2.4.4 Multi-Graphics Controller Multi-Monitor Support

The processor supports simultaneous use of the Processor Graphics Controller (GT) and a x16 PCI Express Graphics (PEG) device.

The processor supports a maximum of 2 displays connected to the PEG card in parallel with up to 2 displays connected to the PCH.

Note: When supporting Multi Graphics controllers Multi-Monitors, "drag and drop" between monitors and the 2x8 PEG is not supported.

2.5 Platform Environment Control Interface (PECI)

The PECI is a one-wire interface that provides a communication channel between a PECI client (processor) and a PECI master. The processor implements a PECI interface to:

- Allow communication of processor thermal and other information to the PECI master.
- Read averaged Digital Thermal Sensor (DTS) values for fan speed control.

2.6 Interface Clocking

2.6.1 Internal Clocking Requirements

Table 2-4. Reference Clock

§ §

Interfaces

3 Technologies

This chapter provides a high-level description of Intel technologies implemented in the processor.

The implementation of the features may vary between the processor SKUs.

Details on the different technologies of Intel processors and other relevant external notes are located at the Intel technology web site: http://www.intel.com/technology/

3.1 Intel® Virtualization Technology (Intel® VT)

Intel Virtualization Technology (Intel[®] VT) makes a single system appear as multiple independent systems to software. This allows multiple, independent operating systems to run simultaneously on a single system. Intel VT comprises technology components to support virtualization of platforms based on Intel architecture microprocessors and chipsets. Intel Virtualization Technology (Intel VT-x) added hardware support in the processor to improve the virtualization performance and robustness. Intel Virtualization Technology for Directed I/O (Intel VT-d) adds chipset hardware implementation to support and improve I/O virtualization performance and robustness.

Intel VT-x specifications and functional descriptions are included in the *Intel*® *64 and IA-32 Architectures Software Developer's Manual, Volume 3B* and is available at:

http://www.intel.com/products/processor/manuals/index.htm

The Intel VT-d specification and other VT documents can be referenced at:

http://www.intel.com/technology/virtualization/index.htm

3.1.1 Intel® Virtualization Technology (Intel® VT) for IA-32, Intel® 64 and Intel® Architecture (Intel® VT-x) Objectives

Intel VT-x provides hardware acceleration for virtualization of IA platforms. Virtual Machine Monitor (VMM) can use Intel VT-x features to provide improved a reliable virtualized platform. By using Intel VT-x, a VMM is:

- **Robust:** VMMs no longer need to use paravirtualization or binary translation. This means that they will be able to run off-the-shelf OSs and applications without any special steps.
- **Enhanced:** Intel VT enables VMMs to run 64-bit guest operating systems on IA x86 processors.
- **More reliable:** Due to the hardware support, VMMs can now be smaller, less complex, and more efficient. This improves reliability and availability and reduces the potential for software conflicts.
- **More secure:** The use of hardware transitions in the VMM strengthens the isolation of VMs and further prevents corruption of one VM from affecting others on the same system.

3.1.2 Intel® Virtualization Technology (Intel® VT) for IA-32, Intel® 64 and Intel® Architecture (Intel® VT-x) Features

The processor core supports the following Intel VT-x features:

- Extended Page Tables (EPT)
	- EPT is hardware assisted page table virtualization
	- It eliminates VM exits from guest OS to the VMM for shadow page-table maintenance
- Virtual Processor IDs (VPID)
	- Ability to assign a VM ID to tag processor core hardware structures (such as TLBs)
	- This avoids flushes on VM transitions to give a lower-cost VM transition time and an overall reduction in virtualization overhead.
- Guest Preemption Timer
	- Mechanism for a VMM to preempt the execution of a guest OS after an amount of time specified by the VMM. The VMM sets a timer value before entering a guest
	- The feature aids VMM developers in flexibility and Quality of Service (QoS) assurances
- Descriptor-Table Exiting
	- Descriptor-table exiting allows a VMM to protect a guest OS from internal (malicious software based) attack by preventing relocation of key system data structures like IDT (interrupt descriptor table), GDT (global descriptor table), LDT (local descriptor table), and TSS (task segment selector).
	- A VMM using this feature can intercept (by a VM exit) attempts to relocate these data structures and prevent them from being tampered by malicious software.

3.1.3 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 operating system, 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.

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

The processor supports the following Intel VT-d features:

- Memory controller and Processor Graphics comply with Intel® VT-d 1.2 specification.
- Two VT-d DMA remap engines.
	- iGraphics DMA remap engine
	- DMI/PEG
- Support for root entry, context entry, and default context
- 39-bit guest physical address and host physical address widths
- Support for 4K page sizes only
- Support for register-based fault recording only (for single entry only) and support for MSI interrupts for faults
- Support for both leaf and non-leaf caching
- Support for boot protection of default page table
- Support for non-caching of invalid page table entries
- Support for hardware based flushing of translated but pending writes and pending reads, on IOTLB invalidation
- Support for page-selective IOTLB invalidation
- MSI cycles (MemWr to address FEEx_xxxxh) not translated
	- Translation faults result in cycle forwarding to VBIOS region (byte enables masked for writes). Returned data may be bogus for internal agents, PEG/DMI interfaces return unsupported request status
- Interrupt Remapping is supported
- Queued invalidation is supported.
- VT-d translation bypass address range is supported (Pass Through)
- *Note:* Intel VT-d Technology may not be available on all SKUs.

3.1.5 Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d) Features Not Supported

The following features are not supported by the processor with Intel VT-d:

- No support for PCISIG endpoint caching (ATS)
- No support for Intel VT-d read prefetching/snarfing (that is, translations within a cacheline are not stored in an internal buffer for reuse for subsequent translations).
- No support for advance fault reporting
- No support for super pages
- No support for Intel VT-d translation bypass address range (such usage models need to be resolved with VMM help in setting up the page tables correctly)

3.2 Intel® Trusted Execution Technology (Intel® TXT)

Intel Trusted Execution Technology (Intel TXT) defines platform-level enhancements that provide the building blocks for creating trusted platforms.

The Intel TXT platform helps to provide the authenticity of the controlling environment such that those wishing to rely on the platform can make an appropriate trust decision. The Intel TXT platform determines the identity of the controlling environment by accurately measuring and verifying the controlling software.

Another aspect of the trust decision is the ability of the platform to resist attempts to change the controlling environment. The Intel TXT platform will resist attempts by software processes to change the controlling environment or bypass the bounds set by the controlling environment.

Intel TXT is a set of extensions designed to provide a measured and controlled launch of system software that will then establish a protected environment for itself and any additional software that it may execute.

These extensions enhance two areas:

- The launching of the Measured Launched Environment (MLE)
- The protection of the MLE from potential corruption

The enhanced platform provides these launch and control interfaces using Safer Mode Extensions (SMX).

The SMX interface includes the following functions:

- Measured/Verified launch of the MLE
- Mechanisms to ensure the above measurement is protected and stored in a secure location
- Protection mechanisms that allow the MLE to control attempts to modify itself

For more information, refer to the *Intel® TXT Measured Launched Environment Developer's Guide* in http://www.intel.com/technology/security*.*

3.3 Intel® Hyper-Threading Technology (Intel® HT Technology)

The processor supports Intel[®] Hyper-Threading Technology (Intel[®] HT Technology), that allows an execution core to function as two logical processors. While some execution resources (such as caches, execution units, and buses) are shared, each logical processor has its own architectural state with its own set of general-purpose registers and control registers. This feature must be enabled using the BIOS and requires operating system support.

Intel recommends enabling Intel HT Technology with Microsoft Windows 7*, Microsoft Windows Vista*, Microsoft Windows* XP Professional/Windows* XP Home, and disabling Intel HT Technology using the BIOS for all previous versions of Windows operating systems. For more information on Intel HT Technology, see http://www.intel.com/technology/platform-technology/hyper-threading/.

3.4 Intel® Turbo Boost Technology

Intel® Turbo Boost Technology is a feature that allows the processor core to opportunistically and automatically run faster than its rated operating frequency/render clock if it is operating below power, temperature, and current limits. The Intel Turbo Boost Technology feature is designed to increase performance of both multi-threaded and single-threaded workloads. Maximum frequency is dependant on the SKU and number of active cores. No special hardware support is necessary for Intel Turbo Boost Technology. BIOS and the OS can enable or disable Intel Turbo Boost Technology. Compared with previous generation products, Intel Turbo Boost Technology will increase the ratio of application power to TDP. Thus, thermal solutions and platform cooling that are designed to less than thermal design guidance might experience thermal and performance issues since more applications will tend to run at the maximum power limit for significant periods of time.

Note: Intel Turbo Boost Technology may not be available on all SKUs.

3.4.1 Intel® Turbo Boost Technology Frequency

The processor's rated frequency assumes that all execution cores are running an application at the thermal design power (TDP). However, under typical operation, not all cores are active. Therefore, most applications are consuming less than the TDP at the rated frequency. To take advantage of the available thermal headroom, the active cores can increase their operating frequency.

To determine the highest performance frequency amongst active cores, the processor takes the following into consideration:

- The number of cores operating in the C0 state.
- The estimated current consumption.
- The estimated power consumption.
- The temperature.

Any of these factors can affect the maximum frequency for a given workload. If the power, current, or thermal limit is reached, the processor will automatically reduce the frequency to stay with its TDP limit.

Note: Intel Turbo Boost Technology processor frequencies are only active if the operating system is requesting the P0 state. For more information on P-states and C-states, refer to [Chapter 4, "Power Management"](#page-42-0).

3.4.2 Intel® Turbo Boost Technology Graphics Frequency

Graphics render frequency is selected by the processor dynamically based on graphics workload demand. The processor can optimize both processor and Processor Graphics performance by managing power for the overall package. For the Processor Graphics, this allows an increase in the render core frequency and increased graphics performance for graphics intensive workloads. In addition, during processor intensive workloads when the graphics power is low, the processor core can increase its frequency higher within the package power limit. Enabling Intel Turbo Boost Technology will maximize the performance of the processor core and the graphics render frequency within the specified package power levels.

3.5 Intel® Advanced Vector Extensions (Intel® AVX)

Intel Advanced Vector Extensions (Intel AVX) is the latest expansion of the Intel instruction set. It extends the Intel Streaming SIMD Extensions (Intel SSE) from 128 bit vectors into 256-bit vectors. Intel AVX addresses the continued need for vector floating-point performance in mainstream scientific and engineering numerical applications, visual processing, recognition, data-mining/synthesis, gaming, physics, cryptography and other areas of applications. The enhancement in Intel AVX allows for improved performance due to wider vectors, new extensible syntax, and rich functionality including the ability to better manage, rearrange, and sort data. For more information on Intel AVX, see http://www.intel.com/software/avx

3.6 Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)

The processor supports Advanced Encryption Standard New Instructions (Intel AES-NI) that are a set of Single Instruction Multiple Data (SIMD) instructions that enable fast and secure data encryption and decryption based on the Advanced Encryption Standard (AES). Intel AES-NI are valuable for a wide range of cryptographic applications; such as, applications that perform bulk encryption/decryption, authentication, random number generation, and authenticated encryption. AES is broadly accepted as the standard for both government and industry applications, and is widely deployed in various protocols.

Intel AES-NI consists of six Intel SSE instructions. Four instructions, AESENC, AESENCLAST, AESDEC, and AESDELAST facilitate high performance AES encryption and decryption. The other two, AESIMC and AESKEYGENASSIST, support the AES key expansion procedure. Together, these instructions provide a full hardware for supporting AES, offering security, high performance, and a great deal of flexibility.

3.6.1 PCLMULQDQ Instruction

The processor supports the carry-less multiplication instruction, PCLMULQDQ. PCLMULQDQ is a Single Instruction Multiple Data (SIMD) instruction that computes the 128-bit carry-less multiplication of two, 64-bit operands without generating and propagating carries. Carry-less multiplication is an essential processing component of several cryptographic systems and standards. Hence, accelerating carry-less multiplication can significantly contribute to achieving high speed secure computing and communication.

3.7 Intel® 64 Architecture x2APIC

The x2APIC architecture extends the xAPIC architecture that provides a key mechanism for interrupt delivery. This extension is intended primarily to increase processor addressability.

Specifically, x2APIC:

- Retains all key elements of compatibility to the xAPIC architecture
	- delivery modes
	- interrupt and processor priorities
	- interrupt sources
	- interrupt destination types

- Provides extensions to scale processor addressability for both the logical and physical destination modes
- Adds new features to enhance performance of interrupt delivery
- Reduces complexity of logical destination mode interrupt delivery on link based architectures

The key enhancements provided by the x2APIC architecture over xAPIC are the following:

- Support for two modes of operation to provide backward compatibility and extensibility for future platform innovations
	- In xAPIC compatibility mode, APIC registers are accessed through a memory mapped interface to a 4 KB page, identical to the xAPIC architecture.
	- In x2APIC mode, APIC registers are accessed through Model Specific Register (MSR) interfaces. In this mode, the x2APIC architecture provides significantly increased processor addressability and some enhancements on interrupt delivery.
- Increased range of processor addressability in x2APIC mode
	- Physical xAPIC ID field increases from 8 bits to 32 bits, allowing for interrupt processor addressability up to 4G-1 processors in physical destination mode. A processor implementation of x2APIC architecture can support fewer than 32 bits in a software transparent fashion.
	- Logical xAPIC ID field increases from 8 bits to 32 bits. The 32-bit logical x2APIC ID is partitioned into two sub-fields—a 16-bit cluster ID and a 16-bit logical ID within the cluster. Consequently, $((2^2 20) -16)$ processors can be addressed in logical destination mode. Processor implementations can support fewer than 16 bits in the cluster ID sub-field and logical ID sub-field in a software agnostic fashion.
- More efficient MSR interface to access APIC registers
	- To enhance inter-processor and self directed interrupt delivery as well as the ability to virtualize the local APIC, the APIC register set can be accessed only through MSR based interfaces in the x2APIC mode. The Memory Mapped IO (MMIO) interface used by xAPIC is not supported in the x2APIC mode.
- The semantics for accessing APIC registers have been revised to simplify the programming of frequently-used APIC registers by system software. Specifically, the software semantics for using the Interrupt Command Register (ICR) and End Of Interrupt (EOI) registers have been modified to allow for more efficient delivery and dispatching of interrupts.

The x2APIC extensions are made available to system software by enabling the local x2APIC unit in the "x2APIC" mode. To benefit from x2APIC capabilities, a new Operating System and a new BIOS are both needed, with special support for the x2APIC mode.

The x2APIC architecture provides backward compatibility to the xAPIC architecture and forward extendibility for future Intel platform innovations.

Note: Intel x2APIC technology may not be available on all processor SKUs.

For more information, refer to the *Intel® 64 Architecture x2APIC Specification* at http://www.intel.com/products/processor/manuals/

Technologies

4 Power Management

This chapter provides information on the following power management topics:

- Advanced Configuration and Power Interface (ACPI) States
- Processor Core
- Integrated Memory Controller (IMC)
- PCI Express*
- Direct Media Interface (DMI)
- Processor Graphics Controller

Figure 4-1. Power States

4.1 Advanced Configuration and Power Interface (ACPI) States Supported

The ACPI states supported by the processor are described in this section.

4.1.1 System States

Table 4-1. System States

4.1.2 Processor Core / Package Idle States

Table 4-2. Processor Core / Package State Support

4.1.3 Integrated Memory Controller States

Table 4-3. Integrated Memory Controller States

4.1.4 PCI Express* Link States

Table 4-4. PCI Express* Link States

4.1.5 Direct Media Interface (DMI) States

Table 4-5. Direct Media Interface (DMI) States

4.1.6 Processor Graphics Controller States

Table 4-6. Processor Graphics Controller States

4.1.7 Interface State Combinations

Table 4-7. G, S, and C State Combinations

4.2 Processor Core Power Management

While executing code, Enhanced Intel SpeedStep Technology optimizes the processor's frequency and core voltage based on workload. Each frequency and voltage operating point is defined by ACPI as a P-state. When the processor is not executing code, it is idle. A low-power idle state is defined by ACPI as a C-state. In general, lower power C-states have longer entry and exit latencies.

4.2.1 Enhanced Intel® SpeedStep® Technology

The following are the key features of Enhanced Intel SpeedStep Technology:

- Multiple frequency and voltage points for optimal performance and power efficiency. These operating points are known as P-states.
- Frequency selection is software controlled by writing to processor MSRs. The voltage is optimized based on the selected frequency and the number of active processor cores.
	- $-$ If the target frequency is higher than the current frequency, V_{CC} is ramped up in steps to an optimized voltage. This voltage is signaled by the SVID bus to the voltage regulator. Once the voltage is established, the PLL locks on to the target frequency.
	- If the target frequency is lower than the current frequency, the PLL locks to the target frequency, then transitions to a lower voltage by signaling the target voltage on SVID bus.
	- All active processor cores share the same frequency and voltage. In a multicore processor, the highest frequency P-state requested amongst all active cores is selected.
	- Software-requested transitions are accepted at any time. If a previous transition is in progress, the new transition is deferred until the previous transition is completed.
- The processor controls voltage ramp rates internally to ensure glitch-free transitions.
- Because there is low transition latency between P-states, a significant number of transitions per-second are possible.

4.2.2 Low-Power Idle States

When the processor is idle, low-power idle states (C-states) are used to save power. More power savings actions are taken for numerically higher C-states. However, higher C-states have longer exit and entry latencies. Resolution of C-states occur at the thread, processor core, and processor package level. Thread-level C-states are available if Intel HT Technology is enabled.

Caution: Long term reliability cannot be assured unless all the Low Power Idle States are enabled.

Figure 4-2. Idle Power Management Breakdown of the Processor Cores

Entry and exit of the C-States at the thread and core level are shown in [Figure 4-3](#page-46-0).

Figure 4-3. Thread and Core C-State Entry and Exit

While individual threads can request low power C-states, power saving actions only take place once the core C-state is resolved. Core C-states are automatically resolved by the processor. For thread and core C-states, a transition to and from C0 is required before entering any other C-state.

Table 4-8. Coordination of Thread Power States at the Core Level

Note:

1. If enabled, the core C-state will be C1E if all enabled cores have also resolved a core C1 state or higher.

4.2.3 Requesting Low-Power Idle States

The primary software interfaces for requesting low power idle states are through the MWAIT instruction with sub-state hints and the HLT instruction (for C1 and C1E). However, software may make C-state requests using the legacy method of I/O reads from the ACPI-defined processor clock control registers, referred to as P_LVLx. This method of requesting C-states provides legacy support for operating systems that initiate C-state transitions using I/O reads.

For legacy operating systems, P_LVLx I/O reads are converted within the processor to the equivalent MWAIT C-state request. Therefore, P_LVLx reads do not directly result in I/O reads to the system. The feature, known as I/O MWAIT redirection, must be enabled in the BIOS.

Note: The P_LVLx I/O Monitor address needs to be set up before using the P_LVLx I/O read interface. Each P-LVLx is mapped to the supported MWAIT(Cx) instruction as shown in [Table 4-9.](#page-47-0)

Table 4-9. P_LVLx to MWAIT Conversion

The BIOS can write to the C-state range field of the PMG_IO_CAPTURE MSR to restrict the range of I/O addresses that are trapped and emulate MWAIT like functionality. Any P_LVLx reads outside of this range does not cause an I/O redirection to MWAIT(Cx) like request. They fall through like a normal I/O instruction.

Note: When P_LVLx I/O instructions are used, MWAIT substates cannot be defined. The MWAIT substate is always zero if I/O MWAIT redirection is used. By default, P_LVLx I/O redirections enable the MWAIT 'break on EFLAGS.IF' feature that triggers a wakeup on an interrupt, even if interrupts are masked by EFLAGS.IF.

4.2.4 Core C-states

The following are general rules for all core C-states, unless specified otherwise:

- A core C-State is determined by the lowest numerical thread state (such as Thread 0 requests C1E while Thread 1 requests C3, resulting in a core C1E state). See [Table 4-7.](#page-44-0)
- A core transitions to C0 state when:
	- An interrupt occurs
	- There is an access to the monitored address if the state was entered using an MWAIT instruction
- For core C1/C1E, core C3, and core C6, an interrupt directed toward a single thread wakes only that thread. However, since both threads are no longer at the same core C-state, the core resolves to C0.
- A system reset re-initializes all processor cores.

4.2.4.1 Core C0 State

The normal operating state of a core where code is being executed.

4.2.4.2 Core C1/C1E State

C1/C1E is a low power state entered when all threads within a core execute a HLT or MWAIT(C1/C1E) instruction.

A System Management Interrupt (SMI) handler returns execution to either Normal state or the C1/C1E state. See the *Intel® 64 and IA-32 Architecture Software Developer's Manual, Volume 3A/3B: System Programmer's Guide for more information.*

While a core is in C1/C1E state, it processes bus snoops and snoops from other threads. For more information on C1E, see [Section 4.2.5.2.](#page-50-0)

4.2.4.3 Core C3 State

Individual threads of a core can enter the C3 state by initiating a P_LVL2 I/O read to the P_BLK or an MWAIT(C3) instruction. A core in C3 state flushes the contents of its L1 instruction cache, L1 data cache, and L2 cache to the shared L3 cache, while maintaining its architectural state. All core clocks are stopped at this point. Because the core's caches are flushed, the processor does not wake any core that is in the C3 state when either a snoop is detected or when another core accesses cacheable memory.

4.2.4.4 Core C6 State

Individual threads of a core can enter the C6 state by initiating a P_LVL3 I/O read or an MWAIT(C6) instruction. Before entering core C6, the core will save its architectural state to a dedicated SRAM. Once complete, a core will have its voltage reduced to zero volts. During exit, the core is powered on and its architectural state is restored.

4.2.4.5 C-State Auto-Demotion

In general, deeper C-states such as C6 have long latencies and have higher energy entry/exit costs. The resulting performance and energy penalties become significant when the entry/exit frequency of a deeper C-state is high. Therefore, incorrect or inefficient usage of deeper C-states have a negative impact on power. To increase residency and improve power in deeper C-states, the processor supports C-state autodemotion.

There are two C-State auto-demotion options:

- C6 to C3
- C6/C3 To C1

The decision to demote a core from C6 to C3 or C3/C6 to C1 is based on each core's immediate residency history. Upon each core C6 request, the core C-state is demoted to C3 or C1 until a sufficient amount of residency has been established. At that point, a core is allowed to go into C3/C6. Each option can be run concurrently or individually.

This feature is disabled by default. BIOS must enable it in the PMG_CST_CONFIG_CONTROL register. The auto-demotion policy is also configured by this register.

4.2.5 Package C-States

The processor supports C0, C1/C1E, C3, and C6 power states. The following is a summary of the general rules for package C-state entry. These apply to all package Cstates unless specified otherwise:

- A package C-state request is determined by the lowest numerical core C-state amongst all cores.
- A package C-state is automatically resolved by the processor depending on the core idle power states and the status of the platform components.
	- Each core can be at a lower idle power state than the package if the platform does not grant the processor permission to enter a requested package C-state.
	- The platform may allow additional power savings to be realized in the processor.
	- For package C-states, the processor is not required to enter C0 before entering any other C-state.

The processor exits a package C-state when a break event is detected. Depending on the type of break event, the processor does the following:

- If a core break event is received, the target core is activated and the break event message is forwarded to the target core.
	- If the break event is not masked, the target core enters the core C0 state and the processor enters package C0.
- If the break event was due to a memory access or snoop request.
	- But the platform did not request to keep the processor in a higher package Cstate, the package returns to its previous C-state.
	- And the platform requests a higher power C-state, the memory access or snoop request is serviced and the package remains in the higher power C-state.

Table 4-10. Coordination of Core Power States at the Package Level

Note:

1. If enabled, the package C-state will be C1E if all cores have resolved a core C1 state or higher.

4.2.5.1 Package C0

This is the normal operating state for the processor. The processor remains in the normal state when at least one of its cores is in the C0 or C1 state or when the platform has not granted permission to the processor to go into a low power state. Individual cores may be in lower power idle states while the package is in C0.

4.2.5.2 Package C1/C1E

No additional power reduction actions are taken in the package C1 state. However, if the C1E sub-state is enabled, the processor automatically transitions to the lowest supported core clock frequency, followed by a reduction in voltage.

The package enters the C1 low power state when:

- At least one core is in the C1 state.
- The other cores are in a C1 or lower power state.

The package enters the C1E state when:

- All cores have directly requested C1E using MWAIT(C1) with a C1E sub-state hint.
- All cores are in a power state lower that C1/C1E but the package low power state is limited to C1/C1E using the PMG_CST_CONFIG_CONTROL MSR.
- All cores have requested C1 using HLT or MWAIT(C1) and C1E auto-promotion is enabled in IA32_MISC_ENABLES.

No notification to the system occurs upon entry to C1/C1E.

4.2.5.3 Package C3 State

A processor enters the package C3 low power state when:

- At least one core is in the C3 state.
- The other cores are in a C3 or lower power state, and the processor has been granted permission by the platform.
- The platform has not granted a request to a package C6 state but has allowed a package C6 state.

In package C3-state, the L3 shared cache is valid.

4.2.5.4 Package C6 State

A processor enters the package C6 low power state when:

- At least one core is in the C6 state.
- The other cores are in a C6 or lower power state, and the processor has been granted permission by the platform.

In package C6 state, all cores have saved their architectural state and have had their core voltages reduced to zero volts. The L3 shared cache is still powered and snoopable in this state. The processor remains in package C6 state as long as any part of the L3 cache is active.

4.3 Integrated Memory Controller (IMC) Power Management

The main memory is power managed during normal operation and in low-power ACPI Cx states.

4.3.1 Disabling Unused System Memory Outputs

Any system memory (SM) interface signal that goes to a memory module connector in which it is not connected to any actual memory devices (such as DIMM connector is unpopulated, or is single-sided) is tri-stated. The benefits of disabling unused SM signals are:

- Reduced power consumption.
- Reduced possible overshoot/undershoot signal quality issues seen by the processor I/O buffer receivers caused by reflections from potentially un-terminated transmission lines.

When a given rank is not populated, the corresponding chip select and CKE signals are not driven.

At reset, all rows must be assumed to be populated, until it can be proven that they are not populated. This is due to the fact that when CKE is tristated with an DIMM present, the DIMM is not ensured to maintain data integrity.

SCKE tri-state should be enabled by BIOS where appropriate, since at reset all rows must be assumed to be populated.

4.3.2 DRAM Power Management and Initialization

The processor implements extensive support for power management on the SDRAM interface. There are four SDRAM operations associated with the Clock Enable (CKE) signals that the SDRAM controller supports. The processor drives four CKE pins to perform these operations.

The CKE is one of the power-save means. When CKE is off the internal DDR clock is disabled and the DDR power is reduced. The power-saving differs according the selected mode and the DDR type used. For more information, please refer to the IDD table in the DDR specification.

The DDR specification defines 3 levels of power-down that differ in power-saving and in wakeup time:

- 1. **Active power-down (APD):** This mode is entered if there are open pages when de-asserting CKE. In this mode the open pages are retained. Power-saving in this mode is the lowest. Power consumption of DDR is defined by IDD3P. Exiting this mode is fined by tXP – small number of cycles.
- 2. **Precharged power-down (PPD):** This mode is entered if all banks in DDR are precharged when de-asserting CKE. Power-saving in this mode is intermediate – better than APD, but less than DLL-off. Power consumption is defined by IDD2P1. Exiting this mode is defined by tXP. Difference from APD mode is that when wakingup all page-buffers are empty
- 3. **DLL-off:** In this mode the data-in DLLs on DDR are off. Power-saving in this mode is the best among all power-modes. Power consumption is defined by IDD2P1. Exiting this mode is defined by tXP, but also tXPDLL $(10 - 20$ according to DDR type) cycles until first data transfer is allowed.

The processor supports 5 different types of power-down. The different modes are the power-down modes supported by DDR3 and combinations of these. The type of CKE power-down is defined by the configuration. The are options are:

- 1. No power-down
- 2. APD: The rank enters power-down as soon as idle-timer expires, no matter what is the bank status
- 3. PPD: When idle timer expires the MC sends PRE-all to rank and then enters powerdown
- 4. DLL-off: same as option (2) but DDR is configured to DLL-off
- 5. APD, change to PPD (APD-PPD): Begins as option (1), and when all page-close timers of the rank are expired, it wakes the rank, issues PRE-all, and returns to PPD APD, change to DLL-off (APD_DLLoff) – Begins as option (1), and when all pageclose timers of the rank are expired, it wakes the rank, issues PRE-all and returns to DLL-off power-down

The CKE is determined per rank when it is inactive. Each rank has an idle-counter. The idle-counter starts counting as soon as the rank has no accesses, and if it expires, the rank may enter power-down while no new transactions to the rank arrive to queues. The idle-counter begins counting at the last incoming transaction arrival.

It is important to understand that since the power-down decision is per rank, the MC can find many opportunities to power-down ranks even while running memory intensive applications, and savings are significant (may be a few watts, according to the DDR specification). This is significant when each channel is populated with more ranks.

Selection of power modes should be according to power-performance or thermal tradeoffs of a given system:

- When trying to achieve maximum performance and power or thermal consideration is not an issue: use no power-down.
- In a system that tries to minimize power-consumption, try to use the deepest power-down mode possible – DLL-off or APD_DLLoff.
- In high-performance systems with dense packaging (that is, complex thermal design) the power-down mode should be considered in order to reduce the heating and avoid DDR throttling caused by the heating.

Control of the power-mode through CRB-BIOS: The BIOS selects by default no-powerdown. There are knobs to change the power-down selected mode.

Another control is the idle timer expiration count. This is set through PM_PDWN_config bits 7:0 (MCHBAR +4CB0). As this timer is set to a shorter time, the MC will have more opportunities to put DDR in power-down. The minimum recommended value for this register is 15. There is no BIOS hook to set this register. Customers who choose to change the value of this register can do it by changing the BIOS. For experiments, this register can be modified in real time if BIOS did not lock the MC registers.

Note: In APD, APD-PPD, and APD-DLLoff there is no point in setting the idle-counter in the same range of page-close idle timer.

> Another option associated with CKE power-down is the S_DLL-off. When this option is enabled, the SBR I/O slave DLLs go off when all channel ranks are in power-down. (Do **not** confuse it with the DLL-off mode, in which the **DDR** DLLs are off). This mode requires to define the I/O slave DLL wakeup time.

4.3.2.1 Initialization Role of CKE

During power-up, CKE is the only input to the SDRAM that has its level recognized (other than the DDR3 reset pin) once power is applied. It must be driven LOW by the DDR controller to make sure the SDRAM components float DQ and DQS during powerup. CKE signals remain LOW (while any reset is active) until the BIOS writes to a configuration register. Using this method, CKE is ensured to remain inactive for much longer than the specified 200 micro-seconds after power and clocks to SDRAM devices are stable.

4.3.2.2 Conditional Self-Refresh

Intel Rapid Memory Power Management (Intel RMPM) conditionally places memory into self-refresh in the package C3 and C6 low-power states. Intel RMPM functionality depends on the graphics/display state (relevant only when processor graphics is being used), as well as memory traffic patterns generated by other connected I/O devices. The target behavior is to enter self-refresh as long as there are no memory requests to service.

When entering the S3 – Suspend-to-RAM (STR) state or S0 conditional self-refresh, the processor core flushes pending cycles and then enters all SDRAM ranks into selfrefresh. The CKE signals remain LOW so the SDRAM devices perform self-refresh.

4.3.2.3 Dynamic Power-down Operation

Dynamic power-down of memory is employed during normal operation. Based on idle conditions, a given memory rank may be powered down. The IMC implements aggressive CKE control to dynamically put the DRAM devices in a power-down state. The processor core controller can be configured to put the devices in *active powerdown* (CKE de-assertion with open pages) or *precharge power-down* (CKE de-assertion with all pages closed). Precharge power-down provides greater power savings but has a bigger performance impact, since all pages will first be closed before putting the devices in power-down mode.

If dynamic power-down is enabled, all ranks are powered up before doing a refresh cycle and all ranks are powered down at the end of refresh.

4.3.2.4 DRAM I/O Power Management

Unused signals should be disabled to save power and reduce electromagnetic interference. This includes all signals associated with an unused memory channel. Clocks can be controlled on a per SO-DIMM basis. Exceptions are made for per SO-DIMM control signals such as CS#, CKE, and ODT for unpopulated SO-DIMM slots.

The I/O buffer for an unused signal should be tri-stated (output driver disabled), the input receiver (differential sense-amp) should be disabled, and any DLL circuitry related ONLY to unused signals should be disabled. The input path must be gated to prevent spurious results due to noise on the unused signals (typically handled automatically when input receiver is disabled).

4.4 PCI Express* Power Management

- Active power management support using L0s, and L1 states.
- All inputs and outputs disabled in L2/L3 Ready state.
- *Note:* PEG interface does not support Hot Plug.
- *Note:* Power impact may be observed when PEG link disable power management state is used.

4.5 Direct Media Interface (DMI) Power Management

• Active power management support using L0s/L1 state.

4.6 Graphics Power Management

4.6.1 Intel® Rapid Memory Power Management (Intel® RMPM) (also known as CxSR)

The Intel Rapid Memory Power Management puts rows of memory into self refresh mode during C3/C6 to allow the system to remain in the lower power states longer. Desktop processors routinely save power during runtime conditions by entering the C3, C6 state. Intel RMPM is an indirect method of power saving that can have a significant effect on the system as a whole.

4.6.2 Intel® Graphics Performance Modulation Technology (Intel® GPMT)

Intel Graphics Power Modulation Technology (Intel GPMT) is a method for saving power in the graphics adapter while continuing to display and process data in the adapter. This method will switch the render frequency and/or render voltage dynamically between higher and lower power states supported on the platform based on render engine workload.

In products where Intel® Graphics Dynamic Frequency (also known as Turbo Boost Technology) is supported and enabled, the functionality of Intel GPMT will be maintained by Intel® Graphics Dynamic Frequency (also known as Turbo Boost Technology).

4.6.3 Graphics Render C-State

Render C-State (RC6) is a technique designed to optimize the average power to the graphics render engine during times of idleness of the render engine. Render C-state is entered when the graphics render engine, blitter engine and the video engine have no workload being currently worked on and no outstanding graphics memory transactions. When the idleness condition is met, the Integrated Graphics will program the VR into a low voltage state (\sim 0.4 V) through the SVID bus.

4.6.4 Intel® Smart 2D Display Technology (Intel® S2DDT)

Intel S2DDT reduces display refresh memory traffic by reducing memory reads required for display refresh. Power consumption is reduced by less accesses to the IMC. S2DDT is only enabled in single pipe mode.

Intel S2DDT is most effective with:

- Display images well suited to compression, such as text windows, slide shows, and so on. Poor examples are 3D games.
- Static screens such as screens with significant portions of the background showing 2D applications, processor benchmarks, and so on, or conditions when the processor is idle. Poor examples are full-screen 3D games and benchmarks that flip the display image at or near display refresh rates.

4.6.5 Intel® Graphics Dynamic Frequency

Intel[®] Graphics Dynamic Frequency Technology is the ability of the processor and graphics cores to opportunistically increase frequency and/or voltage above the ensured processor and graphics frequency for the given part. Intel[®] Graphics Dynamic Frequency Technology is a performance feature that makes use of unused package power and thermals to increase application performance. The increase in frequency is determined by how much power and thermal budget is available in the package, and the application demand for additional processor or graphics performance. The processor core control is maintained by an embedded controller. The graphics driver dynamically adjusts between P-States to maintain optimal performance, power, and thermals. The graphics driver will always place the graphics engine in its lowest possible P-State; thereby, acting in the same capacity as Intel GPMT.

4.7 Thermal Power Management

See [Section 4.6](#page-55-0) for all graphics thermal power management-related features.

§ §

Power Management

5 Thermal Management

For thermal specifications and design guidelines, refer to the *2nd Generation Intel® Core™ Processor Family Desktop, Intel® Pentium® Processor Family Desktop, and Intel® Celeron® Processor Family Desktop, and LGA1155 Socket Thermal and Mechanical Specifications and Design Guidelines*.

§ §

Thermal Management

6 Signal Description

This chapter describes the processor signals. They are arranged in functional groups according to their associated interface or category. The following notations are used to describe the signal type.

The signal description also includes the type of buffer used for the particular signal (see [Table 6-1\)](#page-60-0).

Table 6-1. Signal Description Buffer Types

Notes:

1. Qualifier for a buffer type.

6.1 System Memory Interface Signals

Table 6-2. Memory Channel A Signals

Table 6-3. Memory Channel B Signals

6.2 Memory Reference and Compensation Signals

Table 6-4. Memory Reference and Compensation

6.3 Reset and Miscellaneous Signals

Table 6-5. Reset and Miscellaneous Signals

Notes:

1. PCIe bifurcation support varies with the processor and PCH SKUs used.

6.4 PCI Express*-Based Interface Signals

Table 6-6. PCI Express* Graphics Interface Signals

Notes: 1. PE_TX[3:0] and PE_RX[3:0] are only used for platforms that support 20 PCIe lanes.

6.5 Intel® Flexible Display Interface (Intel® FDI) Signals

Table 6-7. Intel® Flexible Display Interface (Intel® FDI)

6.6 Direct Media Interface (DMI) Signals

Table 6-8. Direct Media Interface (DMI) Signals – Processor to PCH Serial Interface

6.7 Phase Lock Loop (PLL) Signals

Table 6-9. Phase Lock Loop (PLL) Signals

6.8 Test Access Points (TAP) Signals

Table 6-10. Test Access Points (TAP) Signals

6.9 Error and Thermal Protection Signals

Table 6-11. Error and Thermal Protection Signals

6.10 Power Sequencing Signals

Table 6-12. Power Sequencing Signals

6.11 Processor Power Signals

Table 6-13. Processor Power Signals

6.12 Sense Signals

Table 6-14. Sense Signals

6.13 Ground and Non-Critical to Function (NCTF) Signals

Table 6-15. Ground and Non-Critical to Function (NCTF) Signals

6.14 Processor Internal Pull-Up / Pull-Down Resistors

Table 6-16. Processor Internal Pull-Up / Pull-Down Resistors

§ §

Signal Description

7 Electrical Specifications

7.1 Power and Ground Lands

The processor has VCC, VDDQ, VCCPLL, VCCSA, VCCAXG, VCCIO and VSS (ground) inputs for on-chip power distribution. All power lands must be connected to their respective processor power planes, while all VSS lands must be connected to the system ground plane. Use of multiple power and ground planes is recommended to reduce I*R drop. The VCC and VCCAXG lands must be supplied with the voltage determined by the processor **S**erial **V**oltage **ID**entification (SVID) interface. A new serial VID interface is implemented on the processor. [Table 7-1](#page-72-0) specifies the voltage level for the various VIDs.

7.2 Decoupling Guidelines

Due to its large number of transistors and high internal clock speeds, the processor is capable of generating large current swings between low- and full-power states. This may cause voltages on power planes to sag below their minimum values, if bulk decoupling is not adequate. Larger bulk storage (C_{BULK}) , such as electrolytic capacitors, supply current during longer lasting changes in current demand (for example, coming out of an idle condition). Similarly, capacitors act as a storage well for current when entering an idle condition from a running condition. To keep voltages within specification, output decoupling must be properly designed.

Caution: Design the board to ensure that the voltage provided to the processor remains within the specifications listed in [Table 7-5.](#page-79-0) Failure to do so can result in timing violations or reduced lifetime of the processor.

7.2.1 Voltage Rail Decoupling

The voltage regulator solution needs to provide:

- bulk capacitance with low effective series resistance (ESR).
- a low interconnect resistance from the regulator to the socket.
- bulk decoupling to compensate for large current swings generated during poweron, or low-power idle state entry/exit.

The power delivery solution must ensure that the voltage and current specifications are met, as defined in [Table 7-5.](#page-79-0)

7.3 Processor Clocking (BCLK[0], BCLK#[0])

The processor uses a differential clock to generate the processor core operating frequency, memory controller frequency, system agent frequencies, and other internal clocks. The processor core frequency is determined by multiplying the processor core ratio by the BCLK frequency. Clock multiplying within the processor is provided by an internal phase locked loop (PLL) that requires a constant frequency input, with exceptions for Spread Spectrum Clocking (SSC).

The processor's maximum non-turbo core frequency is configured during power-on reset by using its manufacturing default value. This value is the highest non-turbo core multiplier at which the processor can operate. If lower maximum speeds are desired, the appropriate ratio can be configured using the FLEX_RATIO MSR.

7.3.1 Phase Lock Loop (PLL) Power Supply

An on-die PLL filter solution is implemented on the processor. Refer to [Table 7-6](#page-81-0) for DC specifications.

7.4 V_{CC} Voltage Identification (VID)

The processor uses three signals for the serial voltage identification interface to support automatic selection of voltages. [Table 7-1](#page-72-0) specifies the voltage level corresponding to the eight bit VID value transmitted over serial VID. A '1' in this table refers to a high voltage level and a '0' refers to a low voltage level. If the voltage regulation circuit cannot supply the voltage that is requested, the voltage regulator must disable itself. VID signals are CMOS push/pull drivers. Refer to [Table 7-9](#page-84-0) for the DC specifications for these signals. The VID codes will change due to temperature and/or current load changes in order to minimize the power of the part. A voltage range is provided in [Table 7-5.](#page-79-0) The specifications are set so that one voltage regulator can operate with all supported frequencies.

Individual processor VID values may be set during manufacturing so that two devices at the same core frequency may have different default VID settings. This is shown in the VID range values in [Table 7-5.](#page-79-0) The processor provides the ability to operate while transitioning to an adjacent VID and its associated voltage. This will represent a DC shift in the loadline.

See the *VR12/IMVP7 SVID Protocol* for further details.

Table 7-1. VR 12.0 Voltage Identification Definition (Sheet 1 of 3)

Table 7-1. VR 12.0 Voltage Identification Definition (Sheet 2 of 3)

Table 7-1. VR 12.0 Voltage Identification Definition (Sheet 3 of 3)

7.5 System Agent (SA) VCC VID

The VCC_{SA} is configured by the processor output pin VCCSA_VID.

VCCSA_VID output default logic state is low for the processors; logic high is reserved for future compatibility.

[Table 7-2](#page-75-0) specifies the different VCCSA_VID configurations.

Table 7-2. VCCSA_VID configuration

Notes:

1. Some of V_{CCSA} configurations are reserved for future Intel processor families.

7.6 Reserved or Unused Signals

The following are the general types of reserved (RSVD) signals and connection guidelines:

- RSVD These signals should not be connected.
- RSVD_NCTF These signals are non-critical to function and may be left unconnected

Arbitrary connection of these signals to V_{CC}, V_{CCIO}, V_{DDQ}, V_{CCPLL}, V_{CCSA,} V_{CCAXG}, V_{SS}, or to any other signal (including each other) may result in component malfunction or incompatibility with future processors. See [Chapter 8](#page-88-0) for a land listing of the processor and the location of all reserved signals.

For reliable operation, always connect unused inputs or bi-directional signals to an appropriate signal level. Unused active high inputs should be connected through a resistor to ground (V_{SS}). Unused outputs maybe left unconnected; however, this may interfere with some Test Access Port (TAP) functions, complicate debug probing, and prevent boundary scan testing. A resistor must be used when tying bi-directional signals to power or ground. When tying any signal to power or ground, a resistor will also allow for system testability. For details see [Table 7-9](#page-84-0).

7.7 Signal Groups

Signals are grouped by buffer type and similar characteristics as listed in [Table 7-3.](#page-76-0) The buffer type indicates which signaling technology and specifications apply to the signals. All the differential signals, and selected DDR3 and Control Sideband signals have On-Die Termination (ODT) resistors. There are some signals that do not have ODT and need to be terminated on the board.

Table 7-3. Signal Groups (Sheet 1 of 2)1

Table 7-3. Signal Groups (Sheet 2 of 2)¹

Notes:

1. Refer to [Chapter 6](#page-60-0) and [Chapter 8](#page-88-0) for signal description details.

2. SA and SB refer to DDR3 Channel A and DDR3 Channel B.

3. The maximum rise/fall time for UNCOREPWRGOOD is 20 ns.

All Control Sideband Asynchronous signals are required to be asserted/de-asserted for at least **10 BCLKs** with a maximum Trise/Tfall of 6 ns for the processor to recognize the proper signal state. See [Section 7.10](#page-79-0) for the DC specifications.

7.8 Test Access Port (TAP) Connection

Due to the voltage levels supported by other components in the Test Access Port (TAP) logic, Intel recommends the processor be first in the TAP chain, followed by any other components within the system. A translation buffer should be used to connect to the rest of the chain unless one of the other components is capable of accepting an input of the appropriate voltage. Two copies of each signal may be required with each driving a different voltage level.

The processor supports Boundary Scan (JTAG) IEEE 1149.1-2001 and IEEE 1149.6- 2003 standards. Some small portion of the I/O pins may support only one of these standards.

7.9 Storage Conditions Specifications

Environmental storage condition limits define the temperature and relative humidity that the device is exposed to while being stored in a moisture barrier bag. The specified storage conditions are for component level prior to board attach.

[Table 7-4](#page-78-0) specifies absolute maximum and minimum storage temperature limits that represent the maximum or minimum device condition beyond which damage, latent or otherwise, may occur. The table also specifies sustained storage temperature, relative humidity, and time-duration limits. These limits specify the maximum or minimum device storage conditions for a sustained period of time. Failure to adhere to the following specifications can affect long term reliability of the processor.

Table 7-4. Storage Condition Ratings

Notes:

- 1. Refers to a component device that is not assembled in a board or socket and is not electrically connected to a voltage reference or I/O signal.
- 2. Specified temperatures are not to exceed values based on data collected. Exceptions for surface mount reflow are specified by the applicable JEDEC standard. Non-adherence may affect processor reliability.
- 3. T_{absolute storage} applies to the unassembled component only and does not apply to the shipping media, moisture barrier bags, or desiccant.
- 4. Component product device storage temperature qualification methods may follow JESD22-A119 (low temp) and JESD22-A103 (high temp) standards when applicable for volatile memory.
- 5. Intel branded products are specified and certified to meet the following temperature and humidity limits that are given as an example only (Non-Operating Temperature Limit: -40 °C to 70 °C and Humidity: 50% to 90%, non-condensing with a maximum wet bulb of 28 °C.) Post board attach storage temperature limits are not specified for non-Intel branded boards.

6. The JEDEC J-JSTD-020 moisture level rating and associated handling practices apply to all moisture sensitive devices removed from the moisture barrier bag.

7. Nominal temperature and humidity conditions and durations are given and tested within the constraints imposed by T_{sustained storage} and customer shelf life in applicable Intel boxes and bags.

7.10 DC Specifications

The processor DC specifications in this section are defined at the processor pads, unless noted otherwise. See [Chapter 8](#page-88-0) for the processor land listings and [Chapter 6](#page-60-0) for signal definitions. Voltage and current specifications are detailed in [Table 7-5,](#page-79-1) [Table 7-6](#page-81-0), and [Table 7-7.](#page-82-0)

The DC specifications for the DDR3 signals are listed in [Table 7-8](#page-83-0) Control Sideband and Test Access Port (TAP) are listed in [Table 7-9](#page-84-0).

[Table 7-5](#page-79-1) through [Table 7-7](#page-82-0) list the DC specifications for the processor and are valid only while meeting the thermal specifications (as specified in the Thermal / Mechanical Specifications and Guidelines), clock frequency, and input voltages. Care should be taken to read all notes associated with each parameter.

7.10.1 Voltage and Current Specifications

Table 7-5. Processor Core Active and Idle Mode DC Voltage and Current Specifications (Sheet 1 of 2)

Table 7-5. Processor Core Active and Idle Mode DC Voltage and Current Specifications (Sheet 2 of 2)

Notes:

- 1. Unless otherwise noted, all specifications in this table are based on estimates and simulations or empirical data. These specifications will be updated with characterized data from silicon measurements at a later date.
- 2. Each processor is programmed with a maximum valid voltage identification value (VID) that is set at manufacturing and cannot be altered. Individual maximum VID values are calibrated during manufacturing such that two processors at the same frequency may have different settings within the VID range. Note that this differs from the VID employed by the processor during a power management event (Adaptive Thermal Monitor, Enhanced Intel SpeedStep Technology, or Low Power States).
- 3. The voltage specification requirements are measured across VCC_SENSE and VSS_SENSE lands at the socket with a 20-MHz bandwidth oscilloscope, 1.5 pF maximum probe capacitance, and 1-MΩ minimum impedance. The maximum length of ground wire on the probe should be less than 5 mm. Ensure external noise from the system is not coupled into the oscilloscope probe.
- 4. ICC_MAX specification is based on the V_{CC} loadline at worst case (highest) tolerance and ripple.
5. The V_{CC} specifications represent static and transient limits.
-
- 6. The loadlines specify voltage limits at the die measured at the VCC_SENSE and VSS_SENSE lands. Voltage regulation feedback for voltage regulator circuits must also be taken from processor VCC_SENSE and VSS_SENSE lands.
- PSx refers to the voltage regulator power state as set by the SVID protocol.
- 8. 2011A (processors with 35 W TDP) loadline slope, TOB, and ripple specifications allow for a cost reduced voltage regulator for boards supporting only the 2011A (processors with 35 W TDP). 2011A (processors with 35 W TDP) processors may also use the loadline slope, TOB, and ripple specifications for the 2011D (processors with 95 W TDP), 2011C (processors with 65 W TDP), and 2011B (processors with 45 W TDP).

Table 7-6. Processor System Agent I/O Buffer Supply DC Voltage and Current Specifications

Notes:

- 1. Unless otherwise noted, all specifications in this table are based on estimates and simulations or empirical data. These specifications will be updated with characterized data from silicon measurements at a later date.
- 2. V_{CCSA} must be provided using a separate voltage source and not be connected to V_{CC}. This specification is measured at VCCSA_SENSE.
measured at VCCSA_SENSE.
3. ±5% total. Minimum of ±2% DC and 3% AC at the sense
-

Table 7-7. Processor Graphics VID based (V_{AXG}) Supply DC Voltage and Current **Specifications**

Notes:

1. V_{CCAXG} is VID based rail.
2. Unless otherwise noted.

2. Unless otherwise noted, all specifications in this table are based on estimates and simulations or empirical data. These specifications will be updated with characterized data from silicon measurements at a later date.

3. The V_{AXG_MIN} and V_{AXG_MAX} loadlines represent static and transient limits.
4. The loadlines specify voltage limits at the die measured at the VAXG_SENSE and VSSAXG_SENSE lands. Voltage regulation feedback for voltage regulator circuits must also be taken from processor VAXG_SENSE and VSSAXG_SENSE lands.

5. PSx refers to the voltage regulator power state as set by the SVID protocol.

6. Each processor is programmed with a maximum valid voltage identification value (VID) that is set at manufacturing and cannot be altered. Individual maximum VID values are calibrated during manufacturing such that two processors at the same frequency may have different settings within the VID range. Note that this differs from the VID employed by the processor during a power management event (Adaptive Thermal Monitor, Enhanced Intel SpeedStep Technology, or Low Power States).

Table 7-8. DDR3 Signal Group DC Specifications

Notes:

1. Unless otherwise noted, all specifications in this table apply to all processor frequencies.
2. V_{IL} is defined as the maximum voltage level at a receiving agent that will be interpreted as a logical low value.

3. V_{IH} is defined as the minimum voltage level at a receiving agent that will be interpreted as a logical high value.

4. V_{IH} and V_{OH} may experience excursions above V_{DDQ}. However, input signal drivers must comply with the signal quality specifications.

5. This is the pull up/down driver resistance.
6. R_{TERM} is the termination on the DIMM and 6. R_{TERM} is the termination on the DIMM and in not controlled by the processor.
7. The minimum and maximum values for these signals are programmable by B

7. The minimum and maximum values for these signals are programmable by BIOS to one of the two sets.
8. DDR3 values are pre-silicon estimations and subject to change.

8. DDR3 values are pre-silicon estimations and subject to change.
9. SM_DRAMPWROK must have a maximum of 15 ns rise or fall tir

SM_DRAMPWROK must have a maximum of 15 ns rise or fall time over V_{DDQ} * 0.55 \pm 200 mV and edge must be monotonic.

Table 7-9. Control Sideband and TAP Signal Group DC Specifications

Notes:

1. Unless otherwise noted, all specifications in this table apply to all processor frequencies.

2. The V_{CCIO} referred to in these specifications refers to instantaneous V_{CCIO}.
3. For V_{IN} between "0" V and V_{CCIO}. Measured when the driver is tristated.

4. V_{IH} and V_{OH} may experience excursions above V_{CCIO} . However, input signal drivers must comply with the signal quality specifications.

Table 7-10. PCI Express* DC Specifications

Notes:

1. Refer to the PCI Express Base Specification for more details.

2. V_{TX-AC-CM-PP} and V_{TX-AC-CM-P} are defined in the PCI Express Base Specification. Measurement is made over at least 10^{\wedge 6} UI.

3. As measured with compliance test load. Defined as $2^*|V_{TXD+} - V_{TXD-}|$.
4. COMP resistance must be provided on the system board with 1% resiste

4. COMP resistance must be provided on the system board with 1% resistors. 5. PEG_ICOMPO, PEG_COMPI, PEG_RCOMPO are the same resistor.

6. RMS value.
7. Measured a 7. Measured at Rx pins into a pair of 50-Ω terminations into ground. Common mode peak voltage is defined by the expression: max{|(Vd+ - Vd-) - V-CMDC|}.

8. DC impedance limits are needed to ensure Receiver detect.

9. The Rx DC Common Mode Impedance must be present when the Receiver terminations are first enabled to ensure that the Receiver Detect occurs properly. Compensation of this impedance can start immediately and the 15 Rx Common Mode Impedance (constrained by RLRX-CM to 50 Ω ±20%) must be within the specified range by the time Detect is entered.

10. Low impedance defined during signaling. Parameter is captured for 5.0 GHz by RLTX-DIFF.

11. These are pre-silicon estimates and are subject to change.

7.11 Platform Environmental Control Interface (PECI) DC Specifications

PECI is an Intel proprietary interface that provides a communication channel between Intel processors and chipset components to external thermal monitoring devices. The processor contains a Digital Thermal Sensor (DTS) that reports a relative die temperature as an offset from Thermal Control Circuit (TCC) activation temperature. Temperature sensors located throughout the die are implemented as analog-to-digital converters calibrated at the factory. PECI provides an interface for external devices to read the DTS temperature for thermal management and fan speed control. More detailed information is provided in the *Platform Environment Control Interface (PECI) Specification*.

7.11.1 PECI Bus Architecture

The PECI architecture based on **wired OR bus** that the clients (as processor PECI) can pull up high (with strong drive).

The idle state on the bus is near zero.

[Figure 7-1](#page-85-0) demonstrates PECI design and connectivity, while the host/originator can be 3rd party PECI host, and one of the PECI clients is the processor PECI device.

Figure 7-1. Example for PECI Host-clients Connection

7.11.2 DC Characteristics

The PECI interface operates at a nominal voltage set by V_{CCIO} . The set of DC electrical specifications shown in [Table 7-11](#page-86-0) is used with devices normally operating from a V_{CCIO} interface supply. V_{CCIO} nominal levels will vary between processor families. All PECI devices will operate at the V_{CCIO} level determined by the processor installed in the system. For specific nominal V_{CCIO} levels, refer to [Table 7-6](#page-81-0).

Table 7-11. PECI DC Electrical Limits

Notes:

1. V_{CCIO} supplies the PECI interface. PECI behavior does not affect V_{CCIO} min/max specifications.
2. The leakage specification applies to powered devices on the PECI bus.
3. The PECI buffer internal pull up res

7.11.3 Input Device Hysteresis

The input buffers in both client and host models must use a Schmitt-triggered input design for improved noise immunity. Use [Figure 7-2](#page-86-1) as a guide for input buffer design.

Figure 7-2. Input Device Hysteresis

Electrical Specifications

8 Processor Pin and Signal Information

8.1 Processor Pin Assignments

The processor pinmap quadrants are shown in [Figure 8-1](#page-89-0) through [Figure 8-4](#page-92-0). [Table 8-1](#page-93-0) provides a listing of all processor pins ordered alphabetically by pin name.

Figure 8-1. Socket Pinmap (Top View, Upper-Left Quadrant)

Figure 8-2. Socket Pinmap (Top View, Upper-Right Quadrant)

'n

Figure 8-3. Socket Pinmap (Top View, Lower-Left Quadrant)

'n

Figure 8-4. Socket Pinmap (Top View, Lower-Right Quadrant)

Pin Name Pin # Buffer Type Dir. BCLK_ITP | C40 | Diff Clk | I BCLK_ITP# D40 Diff Clk I BCLK[0] W2 Diff Clk I BCLK#[0] | W1 | Diff Clk | I BPM#[0] H40 GTL I/O BPM#[1] H38 GTL I/O BPM#[2] G38 GTL I/O BPM#[3] G40 GTL I/O BPM#[4] G39 GTL I/O BPM#[5] F38 GTL I/O BPM#[6] E40 GTL I/O BPM#[7] F40 GTL I/O CATERR# E37 GTL O CFG[0] | H36 | CMOS | I CFG[1] J36 CMOS I CFG[10] M38 CMOS I $CFG[11]$ N36 CMOS I CFG[12] N38 CMOS I CFG[13] | N39 | CMOS | I $CFG[14]$ N37 CMOS I CFG[15] N40 CMOS I $CFG[16]$ $G37$ $CMOS$ I CFG[17] | G36 | CMOS | I CFG[2] J37 CMOS I CFG[3] | K36 | CMOS | I CFG[4] | L36 | CMOS | I CFG[5] N35 CMOS I CFG[6] | L37 | CMOS | I CFG[7] | M36 | CMOS | I CFG[8] **J38** CMOS I CFG[9] | L35 | CMOS | I DBR# | E39 | Async CMOS | O DMI_RX[0] W5 DMI I DMI_RX[1] | V3 | DMI | I DMI_RX[2] | Y3 | DMI | I DMI_RX[3] AA4 DMI I DMI_RX#[0] W4 DMI I DMI_RX#[1] V4 DMI I DMI_RX#[2] Y4 DMI I DMI_RX#[3] AA5 DMI I DMI_TX[0] V7 DMI O DMI_TX[1] W7 DMI O DMI_TX[2] Y6 DMI O DMI_TX[3] AA7 DMI O

Table 8-1. Processor Pin List by Pin Name

Name

Table 8-1. Processor Pin List by Pin Name

Pin

Table 8-1. Processor Pin List by Pin

Table 8-1. Processor Pin List by Pin

DDR3 | I/O DDR3 I/O $DDR3$ I/O $DDR3$ I/O DDR3 I/O $DDR3$ I/O $DDR3$ I/O $DDR3$ I/O $DBR3$ I/O DDR3 I/O $DBR3$ I/O $DDR3$ I/O DDR3 I/O DDR3 I/O DDR3 I/O DDR3 I/O DDR3 | I/O $DDR3$ I/O DDR3 | I/O DDR3 | I/O DDR3 O DDR3 O DDR3 O DDR3 O $DBR3$ O $DBR3$ 0 $DBR3$ O $DBR3$ O DDR3 O $DBR3$ 0 DDR3 O DDR3 O DDR3 O DDR3 O $DBR3$ 0 DDR3 O $DBR3$ 0 DDR3 O $DDR3$ O DDR3 O $DBR3$ O $DDR3$ O $DBR3$ O DDR3 O

Table 8-1. Processor Pin List by Pin Name

Table 8-1. Processor Pin List by Pin Name

SB_BS[2] | AW17 | DDR3 SB_CAS# AK25 DDR3 SB_CK[0] AL21 DDR3 SB_CK[1] AL20 DDR3 SB_CK[2] AL23 DDR3 SB_CK[3] AP21 DDR3 $SB_CK#[0]$ AL22 DDR3

SB_CS#[0] AN25 DDR3 SB_CS#[1] AN26 DDR3 SB_CS#[2] AL25 DDR3 SB_CS#[3] AT26 DDR3 SB_DQ[0] AG7 DDR3 $SB_DQ[1]$ $AG8$ DDR3 $SB_DQ[2]$ $Al9$ DDR3 $SB_DQ[3]$ $Al8$ DDR3 $SB_DQ[4]$ $AG5$ DDR3 SB_DQ[5] AG6 DDR3 SB_DQ[6] AJ6 DDR3 $SB_DQ[7]$ $AJ7$ DDR3 $SB_DQ[8]$ AL7 DDR3 SB_DQ[9] AM7 DDR3 SB_DQ[10] AM10 DDR3 $SB_DQ[11]$ AL10 DDR3 SB_DQ[12] AL6 DDR3 $SB_DQ[13]$ $AM6$ DDR3 $SB_DQ[14]$ AL9 DDR3 $SB_DQ[15]$ $AM9$ DDR3 $SB_DQ[16]$ AP7 DDR3 $SB_DQ[17]$ AR7 DDR3 SB_DQ[18] AP10 DDR3 SB_DQ[19] AR10 DDR3 SB_DQ[20] AP6 DDR3 $SB_DQ[21]$ $AR6$ DDR3 $SB_DQ[22]$ $AP9$ DDR3 SB_DQ[23] AR9 DDR3 SB_DQ[24] AM12 DDR3 $SB_DQ[25]$ $AM13$ DDR3

 $SB_CK#[1]$ $SB_CK#[2]$ $SB_CK#[3]$ $SB_CKE[0]$ $SB_CKE[1]$ $SB_CKE[2]$ SB_CKE[3]

Table 8-1. Processor Pin List by Pin Name

98 Datasheet, Volume 1

Table 8-1. Processor Pin List by Pin Name

Table 8-1. Processor Pin List by Pin

Processor Pin List by Pin Pin Name Pin # Buffer Type Dir.

Table 8-1. Processor Pin List by Pin Name

Table 8-1. Processor Pin List by Pin

Processor Pin List by Pin Name

b<mark>y Pin</mark>

VSS AJ21 GND

VSS AM3 GND

Table 8-1. Processor Pin List by Pin

Table 8-1. Processor Pin List by Pin

<mark>y Pi</mark>n

Table 8-1. Processor Pin List by Pin

Table 8-1. Processor Pin List by Pin

106 Datasheet, Volume 1

Table 8-1. Processor Pin List by Pin Name

§ §

Processor Pin and Signal Information

9 DDR Data Swizzling

To achieve better memory performance and better memory timing, Intel design performed the DDR Data pin swizzling that will allow a better use of the product across different platforms. Swizzling has no effect on functional operation and is invisible to the OS/SW.

However, during debug, swizzling needs to be taken into consideration. This chapter presents swizzling data. When placing a DIMM logic analyzer, the design engineer must pay attention to the swizzling table to perform an efficient memory debug.

Table 9-1. DDR Data Swizzling

Table 9-2. DDR Data Swizzling Table – Channel B

Ξ

§ §

DDR Data Swizzling

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

[Intel](http://www.mouser.com/Intel):

 [LE80536GC0332MS LJ8Z](http://www.mouser.com/access/?pn=LE80536GC0332MS LJ8Z) [CM8062307260237S R058](http://www.mouser.com/access/?pn=CM8062307260237S R058) [CM8062301046704S R05H](http://www.mouser.com/access/?pn=CM8062301046704S R05H) [CM8062301044204S R05Y](http://www.mouser.com/access/?pn=CM8062301044204S R05Y) [CM8062301061600S R05C](http://www.mouser.com/access/?pn=CM8062301061600S R05C) [CM8062301046304S R05R](http://www.mouser.com/access/?pn=CM8062301046304S R05R)

info@moschip.ru

 $\circled{1}$ +7 495 668 12 70

Общество с ограниченной ответственностью «МосЧип» ИНН 7719860671 / КПП 771901001 Адрес: 105318, г.Москва, ул.Щербаковская д.3, офис 1107

Данный компонент на территории Российской Федерации

Вы можете приобрести в компании MosChip.

Для оперативного оформления запроса Вам необходимо перейти по данной ссылке:

http://moschip.ru/get-element

 Вы можете разместить у нас заказ для любого Вашего проекта, будь то серийное производство или разработка единичного прибора.

В нашем ассортименте представлены ведущие мировые производители активных и пассивных электронных компонентов.

Нашей специализацией является поставка электронной компонентной базы двойного назначения, продукции таких производителей как XILINX, Intel (ex.ALTERA), Vicor, Microchip, Texas Instruments, Analog Devices, Mini-Circuits, Amphenol, Glenair.

Сотрудничество с глобальными дистрибьюторами электронных компонентов, предоставляет возможность заказывать и получать с международных складов практически любой перечень компонентов в оптимальные для Вас сроки.

На всех этапах разработки и производства наши партнеры могут получить квалифицированную поддержку опытных инженеров.

Система менеджмента качества компании отвечает требованиям в соответствии с ГОСТ Р ИСО 9001, ГОСТ РВ 0015-002 и ЭС РД 009

Офис по работе с юридическими лицами:

105318, г.Москва, ул.Щербаковская д.3, офис 1107, 1118, ДЦ «Щербаковский»

Телефон: +7 495 668-12-70 (многоканальный)

Факс: +7 495 668-12-70 (доб.304)

E-mail: info@[moschip](mailto:info@moschip.ru).ru

Skype отдела продаж: moschip.ru moschip.ru_4

moschip.ru_6 moschip.ru_9