# Intel® Core™ M Processor Family

## Datasheet – Volume 1 of 2

*September 2014*

Order No.: 330834-001v1

By using this document, in addition to any agreements you have with Intel, you accept the terms set forth below.

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

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.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

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". Intel reserves these for future 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.

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

Any software source code reprinted in this document is furnished for informational purposes only and may only be used or copied and no license, express or implied, by estoppel or otherwise, to any of the reprinted source code is granted by this document.

Any software source code reprinted in this document is furnished under a software license and may only be used or copied in accordance with the terms of that license.

This document contains information on products in the design phase of development.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families: Go to: http://www.intel.com/products/processor_number

Code Names are only for use by Intel to identify products, platforms, programs, services, etc. ("products") in development by Intel that have not been made commercially available to the public, i.e., announced, launched or shipped. They are never to be used as "commercial" names for products. Also, they are not intended to function as trademarks.

Intel® Hyper-Threading Technology (Intel® HT Technology) is available on select Intel® Core™ processors. It requires an Intel® HT Technology enabled system. Consult your PC manufacturer. Performance will vary depending on the specific hardware and software used. Not available on Intel® Core™ i5-750. For more information including details on which processors support Intel® HT Technology, visit http://www.intel.com/info/hyperthreading.

Intel® 64 architecture requires a system with a 64-bit enabled processor, chipset, BIOS and software. Performance will vary depending on the specific hardware and software you use. Consult your PC manufacturer for more information. For more information, visit http://www.intel.com/content/www/us/en/architecture-and-technology/microarchitecture/intel-64-architecture-general.html.

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit http://www.intel.com/technology/security.

Intel® Virtualization Technology (Intel® VT) requires a computer system with an enabled Intel® processor, BIOS, and virtual machine monitor (VMM). Functionality, performance or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit http://www.intel.com/go/virtualization.

Requires a system with Intel® Turbo Boost Technology. Intel Turbo Boost Technology and Intel Turbo Boost Technology 2.0 are only available on select Intel® processors. Consult your PC manufacturer. Performance varies depending on hardware, software, and system configuration. For more information, visit http://www.intel.com/go/turbo.

Requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup and configuration.

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

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

Copyright © –2014, Intel Corporation. All rights reserved.

# Contents

## Figures

# Tables

# Revision History

| Revision | Description | Date |
|---|---|---|
| 001 | • Initial Release | September 2014 |

# 1.0 Introduction

The Intel® Core™ M processor family based on Y-Processor line are 64-bit, multi-core processors built on 14-nanometer process technology.

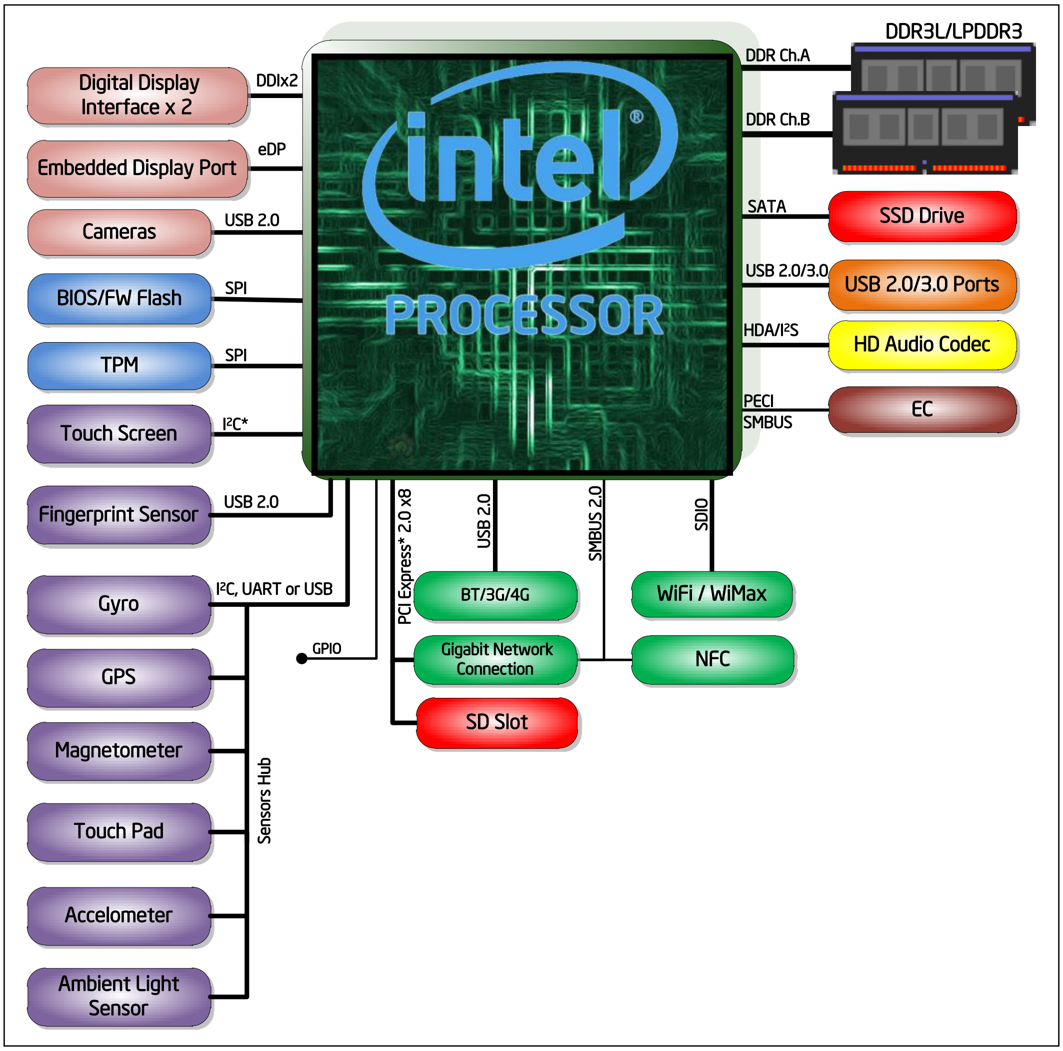
The processors are designed for a one-chip platform that includes a low-power Platform Controller Hub (PCH) die in the same package as the processor die. The PCH is referred to as the Intel® Core™ M Processor Family I/O . See the following figure.

Throughout this document, the Intel® Core™ M processor may be referred to simply as "processor". The Intel® Core™ M processor may also be referred to as "Y-Processor Line".

Throughout this document, the Intel® Core™ M processor family refers to the 5Y10, 5Y10A and 5Y70 processors.

Refer to the processor Specification Update document for additional SKU details.

## Figure 1. Processor Platform Block Diagram



## 1.1 Supported Technologies

- Intel® Virtualization Technology (Intel® VT)
- Intel® Active Management Technology 10.0 (Intel® AMT 10)
- Intel® Trusted Execution Technology (Intel® TXT)
- Intel® Streaming SIMD Extensions 4.2 (Intel® SSE4.2)
- Intel® Hyper-Threading Technology (Intel® HT Technology)
- Intel® 64 Architecture
- Execute Disable Bit
- Intel® Turbo Boost Technology 2.0
- Intel® Advanced Vector Extensions 2.0 (Intel® AVX2)

- Intel® Device Protection Technology with Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)
- PCLMULQDQ Instruction
- Intel® Device Protection Technology with Intel® Secure Key
- PAIR – Power Aware Interrupt Routing
- SMEP – Supervisor Mode Execution Protection
- SMAP – Supervisor Mode Access Protection
- Intel® Device Protection Technology with Boot Guard
- DRAM Bit-Error Recovery (DBER)

*Note:* The availability of the features may vary between processor SKUs.

## 1.2 Power Management Support

### Processor Core

- Full support of ACPI C-states as implemented by the following processor C-states:
  - C0, C1, C1E, C3, C6, C7, C8, C9, C10
- Enhanced Intel SpeedStep® Technology

### System

- S0, S3, S4, S5

### Memory Controller

- Conditional self-refresh
- Dynamic power-down

### Processor Graphics Controller

- Intel® Rapid Memory Power Management (Intel® RMPM)
- Intel® Smart 2D Display Technology (Intel® S2DDT)
- Graphics Render C-state (RC6)
- Intel® Seamless Display Refresh Rate Switching with eDP port
- Intel® Display Power Saving Technology (Intel® DPST)

## 1.3 Thermal Management Support

- Digital Thermal Sensor
- Adaptive Thermal Monitor
- THERMTRIP# and PROCHOT# support
- On-Demand Mode
- Memory Open and Closed Loop Throttling
- Memory Thermal Throttling
- External Thermal Sensor (TS-on-DIMM and TS-on-Board)

- Render Thermal Throttling
- Fan speed control with DTS

## 1.4 Package Support

The processor is available in the following packages:

- Y-Processor Line: 30 mm x 16.5 mm x 1.05 mm BGA package (BGA1234)

## 1.5 Processor Testability

The processor includes boundary-scan for board and system level testability.

## 1.6 Terminology

### Table 1. Terminology

| Term | Description |
|---|---|
| APD | Active Power-down |
| B/D/F | Bus/Device/Function |
| BGA | Ball Grid Array |
| BLC | Backlight Compensation |
| BLT | Block Level Transfer |
| BMP | Binary Modification Program |
| BPP | Bits per pixel |
| CKE | Clock Enable |
| CLTM | Closed Loop Thermal Management |
| DDI | Digital Display Interface |
| DDR3 | Third-generation Double Data Rate SDRAM memory technology |
| DDR3L | DDR3 Low Voltage |
| DDR3L-RS | DDR3 Low Voltage Reduced Standby Power |
| DLL | Delay-Locked Loop |
| DMA | Direct Memory Access |
| DP | DisplayPort* |
| DTS | Digital Thermal Sensor |
| EC | Embedded Controller |
| ECC | Error Correction Code |
| eDP* | embedded DisplayPort* |
| EPG | Electrical Power Gating |
| EU | Execution Unit |
| FMA | Floating-point fused Multiply Add instructions |
| FSC | Fan Speed Control |

*continued...*

| Term | Description |
|---|---|
| HDCP | High-bandwidth Digital Content Protection |
| HDMI* | High Definition Multimedia Interface |
| HFM | High Frequency Mode |
| iDCT | Inverse Discrete |
| IHS | Integrated Heat Spreader |
| GFX | Graphics |
| GUI | Graphical User Interface |
| IMC | Integrated Memory Controller |
| Intel® 64 Technology | 64-bit memory extensions to the IA-32 architecture |
| Intel® DPST | Intel Display Power Saving Technology |
| Intel® TSX-NI | Intel Transactional Synchronization Extensions - New Instructions |
| Intel® TXT | Intel Trusted Execution Technology |
| Intel® VT | Intel Virtualization Technology. Processor virtualization, when used in conjunction with Virtual Machine Monitor software, enables multiple, robust independent software environments inside a single platform. |
| Intel® VT-d | Intel Virtualization Technology (Intel VT) for Directed I/O. Intel VT-d is a hardware assist, under system software (Virtual Machine Manager or OS) control, for enabling I/O device virtualization. Intel VT-d also brings robust security by providing protection from errant DMAs by using DMA remapping, a key feature of Intel VT-d. |
| IOV | I/O Virtualization |
| ISI | Inter-Symbol Interference |
| ITPM | Integrated Trusted Platform Module |
| LFM | Low Frequency Mode. LFM is Pn in the P-state table. It can be read at MSR CEh [47:40]. |
| LFP | Local Flat Panel |
| LPDDR3 | Low-Power Third-generation Double Data Rate SDRAM memory technology |
| MCP | Multi-Chip Package |
| MFM | Minimum Frequency Mode. MFM is the minimum ratio supported by the processor and can be read from MSR CEh [55:48]. |
| MLE | Measured Launched Environment |
| MLC | Mid-Level Cache |
| MSI | Message Signaled Interrupt |
| MSL | Moisture Sensitive Labeling |
| MSR | Model Specific Registers |
| NCTF | Non-Critical to Function. NCTF locations are typically redundant ground or non-critical reserved, so the loss of the solder joint continuity at end of life conditions will not affect the overall product functionality. |
| ODT | On-Die Termination |
| OLTM | Open Loop Thermal Management |

***continued...***

| Term | Description |
|---|---|
| PCG | Platform Compatibility Guide (PCG) (previously known as FMB) provides a design target for meeting all planned processor frequency requirements. |
| PCH | Platform Controller Hub. The chipset with centralized platform capabilities including the main I/O interfaces along with display connectivity, audio features, power management, manageability, security, and storage features. |
| PECI | The Platform Environment Control Interface (PECI) is a one-wire interface that provides a communication channel between Intel processor and chipset components to external monitoring devices. |
| PL1, PL2 | Power Limit 1 and Power Limit 2 |
| PPD | Pre-charge Power-down |
| Processor | The 64-bit multi-core component (package) |
| Processor Core | The term "processor core" refers to Si die itself, which can contain multiple execution cores. Each execution core has an instruction cache, data cache, and 256-KB L2 cache. All execution cores share the L3 cache. |
| Processor Graphics | Intel Processor Graphics |
| Rank | A unit of DRAM corresponding to four to eight devices in parallel, ignoring ECC. These devices are usually, but not always, mounted on a single side of a SO-DIMM. |
| SCI | System Control Interrupt. SCI is used in the ACPI protocol. |
| SDP | Scenario Design Power |
| SF | Strips and Fans |
| SMM | System Management Mode |
| SMX | Safer Mode Extensions |
| Storage Conditions | A non-operational state. The processor may be installed in a platform, in a tray, or loose. Processors may be sealed in packaging or exposed to free air. Under these conditions, processor landings should not be connected to any supply voltages, have any I/Os biased, or receive any clocks. Upon exposure to "free air" (that is, unsealed packaging or a device removed from packaging material), the processor must be handled in accordance with moisture sensitivity labeling (MSL) as indicated on the packaging material. |
| SVID | Serial Voltage Identification |
| TAC | Thermal Averaging Constant |
| TAP | Test Access Point |
| $T_{CASE}$ | The case temperature of the processor, measured at the geometric center of the top-side of the TTV IHS. |
| TCC | Thermal Control Circuit |
| $T_{CONTROL}$ | $T_{CONTROL}$ is a static value that is below the TCC activation temperature and used as a trigger point for fan speed control. When DTS > $T_{CONTROL}$, the processor must comply to the TTV thermal profile. |
| TDP | Thermal Design Power: Thermal solution should be designed to dissipate this target power level. TDP is not the maximum power that the processor can dissipate. |
| TLB | Translation Look-aside Buffer |
| TTV | Thermal Test Vehicle. A mechanically equivalent package that contains a resistive heater in the die to evaluate thermal solutions. |
| TM | Thermal Monitor. A power reduction feature designed to decrease temperature after the processor has reached its maximum operating temperature. |

*continued...*

| Term | Description |
|---|---|
| $V_{CC}$ | Processor core power supply |
| $V_{DDQ}$ | DDR3L and LPDDR3 power supply. |
| VF | Vertex Fetch |
| VID | Voltage Identification |
| VS | Vertex Shader |
| VLD | Variable Length Decoding |
| VMM | Virtual Machine Monitor |
| VR | Voltage Regulator |
| $V_{SS}$ | Processor ground |

## 1.7 Related Documents

### Table 2. Related Documents

| Document | Document Number / Location |
|---|---|
| Intel® Core™ M Processor Family Datasheet, Volume 2 of 2 | 330835 |
| Intel® Core™ M Processor Family Specification Update | 330836 |
| Intel® Core™ M Processor Family I/O Datasheet | 330837 |
| Intel® Core™ M Processor Family I/O Specification Update | 330838 |
| *Advanced Configuration and Power Interface 3.0* | http://www.acpi.info/ |
| *DDR3 SDRAM Specification* | http://www.jedec.org |
| *Low Power Double Data Rate 3 Specification* | http://www.jedec.org |
| *DisplayPort* Specification* | http://www.vesa.org |
| *Intel® 64 and IA-32 Architectures Software Developer's Manuals* | http://www.intel.com/products/processor/manuals/index.htm |

# 2.0 Interfaces

## 2.1 System Memory Interface

### 2.1.1 System Memory Technology Supported

The processor system memory controller supports DDR3L, DDR3L-RS, LPDDR3 memory technologies with the following features and details.

**Table 3. Supported Memory Technology Details**

| Parameter | | Details | | Notes |
|---|---|---|---|---|
| **Processor Type** | | **Y-Processor Line** | | |
| Memory Type | | DDR3L, DDR3L-RS | LPDDR3 | 1 |
| Connector/Memory Down | | Memory Down | Memory Down | |
| System Memory I/O Voltage | | 1.35V | 1.20V | |
| Transfer Rate (MT/s) | | 1333 and 1600 | 1600 | |
| Channels | | 1 and 2 | 1 and 2 | |
| DIMMs Per Channel | | N/A | N/A | |
| Maximum Ranks Per Channel | | 2 | 2 | |
| DRAM Die Density (Gb) | | 2 and 4 | 4 | |
| Max Capacity (GB) | | 8 | 8 | 8 |
| Theoretical Maximum Bandwidth (GB/s) | 1333 | 21.3 | N/A | 9 |
| | 1600 | 25.6 | 25.6 | |
| DIMM Raw Card (RC)<br>Down (Pkg Ranks – Die bits – Pkg bits) Types | | 96-Ball BGA<br>SDP 1-16-16<br>DDP 2-16-16 | 178-Ball BGA<br>SDP 1-32-32<br>DDP 2-32-32<br>QDP 2-16-32 | 2, 3 |
| ECC | | No | No | |
| On-Die Termination (ODT) Signals | | Disabled | Disabled | |
| Command Mode | | 1N and 2N | 0.5N | 4 |
| CPU System Memory Ballmap | | Non-interleaved | Non-interleaved | 5 |
| tCL-tRCD-tRP-CWL (tCK) | 1333 | 8-8-8-7 , 9-9-9-7 | 10-12-12-7 | 6 |
| | 1600 | 10-10-10-8, 11-11-11-8 | 12-15-15-8 | 6 |
| DRAM Reference Voltage Generation | | VREF_DQ, VREF_CA | VREF_DQ, VREF_CA | 7 |
| Data Bus Width (bits) | | 64 | 64 | |

*continued...*

| Parameter | Details | | Notes |
|---|---|---|---|
| Processor Type | Y-Processor Line | | |
| Data Burst Length | 8 | 8 | |
| DRAM Device Bank Support | 8 | 8 | |

*Notes:* 1. DDR3L = Low Voltage Double Data Rate 3, DDR3L-RS = Low Voltage Double Data Rate 3 Reduced Stand-by, LPDDR3 = Low Power Double Data Rate 3

2. Raw Card A = Dual Ranked x16 unbuffered, Raw Card B = Single Ranked x8 unbuffered, Raw Card C = Single Ranked x16 unbuffered, Raw Card F = Dual Ranked x8 unbuffered
3. SDP = Single Die Package, DDP = Dual Die Package, QDP = Quad Die Package
4. Command 0.5N Mode indicates a new command may be transferred on both the positive and negative edges of the clock, Command 1N Mode indicates a new command may be issued every clock, and Command 2N Mode indicates a new command may be issued every 2 clocks.
5. The side-by-side ball map placement, also called "Non-Interleaved", where each memory channel's DQ/DQS/DQS# signals are grouped together on one side of the processor package. Interleaved processor Memory ball map is where the Channel 0 strobe and data balls are grouped along the outer perimeter and the Channel 1 strobe and data balls are grouped along the inner part of the ball map.
6. tCL = CAS Latency, tRCD = Activate Command to READ or WRITE Command delay, tRP = PRECHARGE Command Period, CWL = CAS Write Latency, tCK = Clock Cycle
7. The System Memory Controller generated DRAM device side Reference Voltage for the DQ Input Receivers (VREFDQ) and the Reference Voltage for the Command and Control Input Receivers (VREFCA) for both system memory interface channels.
8. Max Capacity (GB) = (DRAM Die Gb Technology * Total Number of DRAM Dies) / 8
   a. Memory Down Example:
      i. Channel A = LPDDR3 QDP 2-16-32 = 2 QDP DRAM 16Gb Packages = 8 Total DRAM 4Gb Dies
      ii. Channel B = LPDDR3 QDP 2-16-32 = 2 QDP DRAM 16Gb Packages = 8 Total DRAM 4Gb Dies
      iii. Maximum Capacity (GB) = ( 4Gb * (8 + 8) ) / 8 = 8 GB
9. Theoretical Maximum Bandwidth (GB/s) = ( ( Transfer Rate * Number of Memory Channels * Channel Data Bits ) / 8 ) / 1000
   a. 1333 Example: = ( ( 1333 * 2 * 64 ) / 8 ) / 1000 = 21.3 GB/s
   b. 1600 Example: = ( ( 1600 * 2 * 64 ) / 8 ) / 1000 = 25.6 GB/s

## 2.1.2 System Memory Organization Modes

The system memory controller supports two memory organization modes – single-channel and dual-channel. Depending on how the DIMM Modules or DRAM Down Devices are configured in each memory channel, a number of different configurations can exist.

### Single-Channel Mode

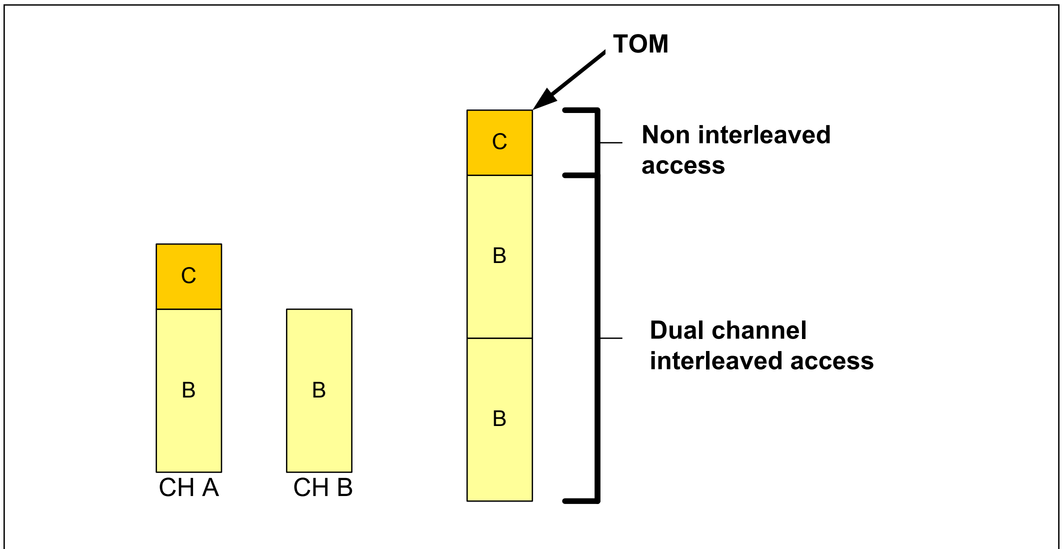
In this mode, all memory cycles are directed to a single-channel. Single-channel mode is used when either Channel A or Channel B are populated in any order, but not both.

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

The system memory controller supports Intel Flex Memory Technology Mode where memory is divided into a symmetric and 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 entire memory array. This mode is used when both Channel A and Channel B are populated with memory but the total amount of memory in each channel is not the same.

*Note:* Channels A and B can be mapped for Physical Channel 0 and 1 respectively or vice versa; however, the Channel A size must be greater or equal to the Channel B size.

**Figure 2. Intel® Flex Memory Technology Operations**



CH A and CH B can be configured to be physical channels 0 or 1
B – The largest physical memory amount of the smaller size memory module
C – The remaining physical memory amount of the larger size memory module

### 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. This mode is used when both Channel A and Channel B are populated with the same amount of total memory.

## 2.1.3 Intel® Fast Memory Access (Intel® FMA)

### Just-in-Time Command Scheduling

The system 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, the requests 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.

### Command Overlap

Command Overlap allows the insertion of the DRAM commands between the Activate, Pre-charge, 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.

### Out-of-Order Scheduling

While leveraging the Just-in-Time Scheduling and Command Overlap enhancements, the system memory controller 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 system memory controller to further reduce latency and increase bandwidth efficiency.

### 2.1.4 Data Scrambling

The system memory controller incorporates a Data Scrambling feature to minimize the impact of excessive di/dt on the platform system memory 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, which is generally limited by data patterns that excite resonance between the package inductance and on die capacitances. As a result, the system memory controller uses a data scrambling feature to create pseudo-random patterns on the system memory data bus to reduce the impact of any excessive di/dt.

## 2.2 Processor Graphics

The processor graphics contains a generation 8 graphics core architecture. This enables substantial gains in performance and lower power consumption over previous generations.

- 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 (1.4a specification compliant with 3D)
- DirectX* Video Acceleration (DXVA) support for accelerating video processing
  - Full AVC/VC1/MPEG2 HW Decode
- Scalable Video Codec (SVC) Decode/Encode HW Acceleration
  - Extension of H.264 format
  - Single video stream with multiple subset bit streams or enhancement layers
- VP8* Decode HW Acceleration
  - Open Source Codec
  - Full HW Acceleration for decode support
- Advanced Scheduler 2.0, 1.0, XPDM support
- Windows* 8, Windows* 7, OSX, Linux* operating system support
- DirectX* 11.1, DirectX* 11.1+, DirectX* 11, DirectX* 10.1, DirectX* 10, DirectX* 9 support.
- OpenGL* 4.0, OpenGL* 4.2 support

## 2.3 Processor Graphics Controller (GT)

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

The Display Engine 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.

### 2.3.1 3D and Video Engines for Graphics Processing

The Gen 8 engine provides the following performance and power-management enhancements.

#### 3D Pipeline

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.

#### 3D Engine Execution Units

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

#### 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*.

#### 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.

#### 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.

#### 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.

### 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.

### 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.

### Video Engine

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

### 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.

### 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 x 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.

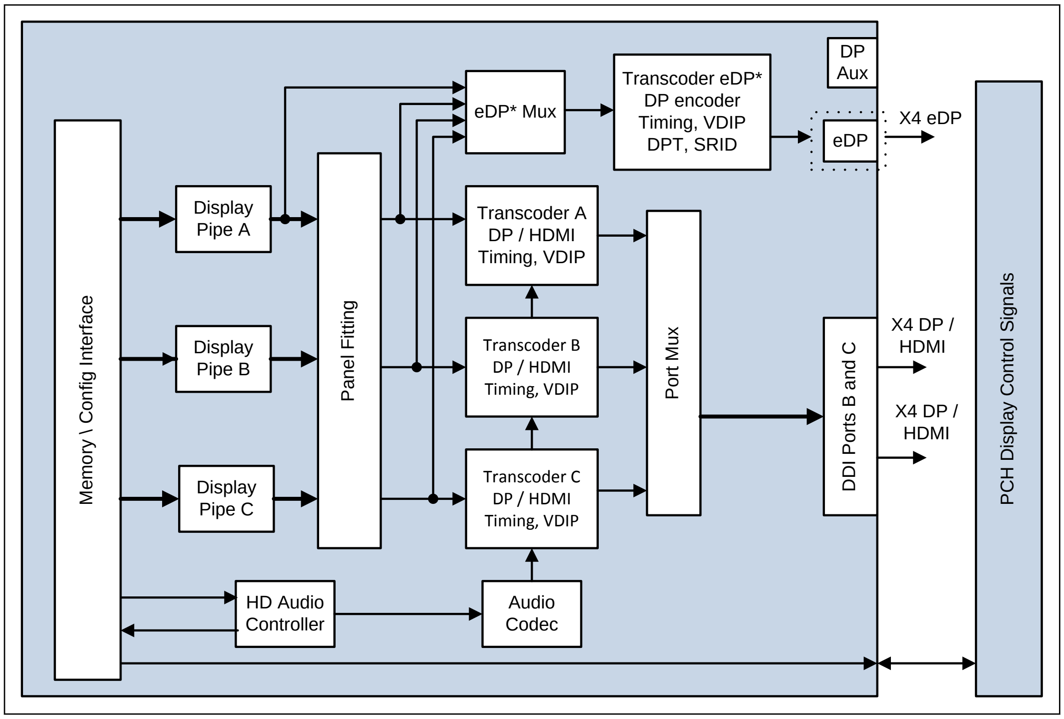
Data is horizontally and vertically aligned at the destination. If the destination for the BLT overlaps with the source memory location, the BLT engine specifies which area in memory to begin the BLT transfer. Hardware is included for all 256 raster operations (source, pattern, and destination) defined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

- The processor supports:
  - — Two Digital Display (x4 DDI) interfaces that can be configured as DisplayPort*, HDMI*. The DisplayPort* can be configured to use 1, 2, or 4 lanes depending on the bandwidth requirements and link data rate of RBR (1.62 GT/s), HBR (2.97 GT/s), and HBR2 (5.4 GT/s). When configured as HDMI*, the DDIx4 port can support 2.97 GT/s.
  - — One dedicated x4 embedded DisplayPort* (eDP*). Built-in displays are only supported on eDP.
- The HDMI* interface supports HDMI with 3D, 4K, Deep Color, and x.v.Color. The DisplayPort* interface supports the VESA DisplayPort* Standard Version 1, Revision 2.
- The processor supports High-bandwidth Digital Content Protection (HDCP) for high-definition content playback over digital interfaces.
- The processor also integrates dedicated a Mini HD audio controller to drive audio on integrated digital display interfaces, such as HDMI* and DisplayPort*. The HD audio controller on the PCH would continue to support down CODECs, and so on. The processor Mini HD audio controller supports two High-Definition Audio streams simultaneously on any of the three digital ports.
- The processor supports streaming any 3 independent and simultaneous display combination of DisplayPort*/HDMI*/eDP*/ monitors. In the case of 3 simultaneous displays, two High Definition Audio streams over the digital display interfaces are supported.
- Each digital port is capable of driving resolutions up to 3840x2160 at 60 Hz using 4 lanes at link data rate HBR2 through DisplayPort* and 4096x2304 at 24 Hz using HDMI*. Use of active level shifter is required to obtain maximum HDMI resolution.
- DisplayPort* Aux CH, DDC channel, Panel power sequencing, and HPD are supported through the PCH.

## Figure 3. Processor Display Architecture


Memory \ Config Interface
Display Pipe A
Display Pipe B
Display Pipe C
Panel Fitting
eDP* Mux
Transcoder eDP* DP encoder Timing, VDIP DPT, SRID
DP Aux
eDP
X4 eDP
Transcoder A DP / HDMI Timing, VDIP
Transcoder B DP / HDMI Timing, VDIP
Transcoder C DP / HDMI Timing, VDIP
Port Mux
DDI Ports B and C
X4 DP / HDMI
X4 DP / HDMI
PCH Display Control Signals
HD Audio Controller
Audio Codec

Display is the presentation stage of graphics. This involves:

- Pulling rendered data from memory
- Converting raw data into pixels
- Blending surfaces into a frame
- Organizing pixels into frames
- Optionally scaling the image to the desired size
- Re-timing data for the intended target
- Formatting data according to the port output standard

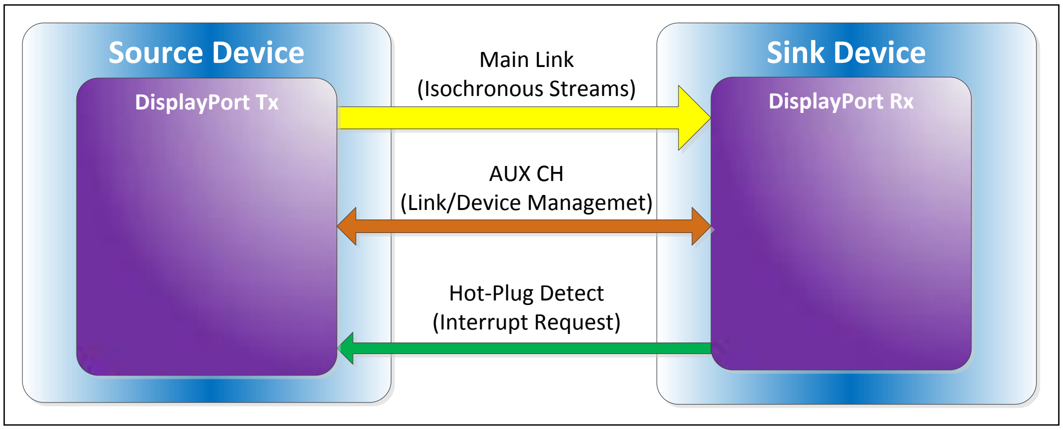
### DisplayPort*

DisplayPort* is a digital communication interface that uses differential signaling to achieve a high-bandwidth bus interface designed to support connections between PCs and monitors, projectors, and TV displays.

A DisplayPort* consists of a Main Link, Auxiliary channel, and a Hot-Plug Detect signal. The Main Link is a unidirectional, high-bandwidth, and low latency channel used for transport of isochronous data streams such as uncompressed video and audio. The Auxiliary Channel (AUX CH) is a half-duplex bidirectional channel used for link management and device control. The Hot-Plug Detect (HPD) signal serves as an interrupt request for the sink device.

The processor is designed in accordance with the VESA DisplayPort* Standard Version 1.2a. The processor supports *VESA DisplayPort* PHY Compliance Test Specification 1.2a* and *VESA DisplayPort* Link Layer Compliance Test Specification 1.2a*.

Figure 4. DisplayPort* Overview



## High-Definition Multimedia Interface (HDMI*)

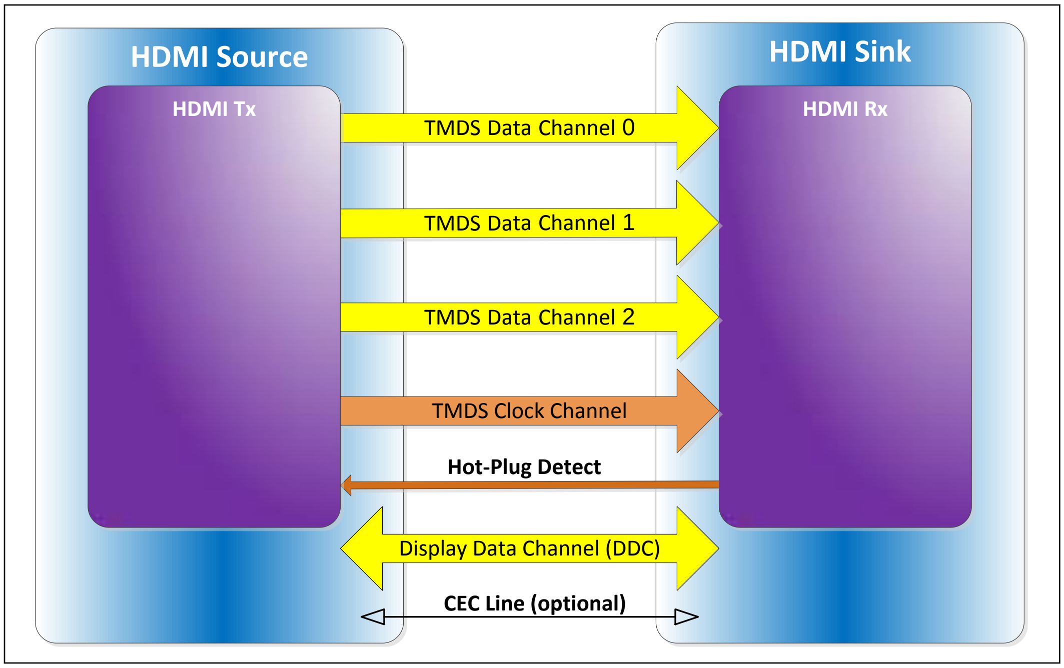
The High-Definition Multimedia Interface* (HDMI*) is provided for transmitting uncompressed digital audio and video signals from DVD players, set-top boxes, and other audiovisual sources to television sets, projectors, and other video displays. It can carry high quality multi-channel audio data and all standard and high-definition consumer electronics video formats. The HDMI display interface connecting the processor and display devices uses transition minimized differential signaling (TMDS) to carry audiovisual information through the same HDMI cable.

HDMI includes three separate communications channels — TMDS, DDC, and the optional CEC (consumer electronics control). CEC is not supported on the processor. As shown in the following figure, the HDMI cable carries four differential pairs that make up the TMDS data and clock channels. These channels are used to carry video, audio, and auxiliary data. In addition, HDMI carries a VESA DDC. The DDC is used by an HDMI Source to determine the capabilities and characteristics of the Sink.

Audio, video, and auxiliary (control/status) data is transmitted across the three TMDS data channels. The video pixel clock is transmitted on the TMDS clock channel and is used by the receiver for data recovery on the three data channels. The digital display data signals driven natively through the PCH are AC coupled and needs level shifting to convert the AC coupled signals to the HDMI compliant digital signals.

The processor HDMI interface is designed in accordance with the High-Definition Multimedia Interface with 3D, 4K, Deep Color, and x.v.Color.

### Figure 5. HDMI* Overview



### embedded DisplayPort*

The embedded DisplayPort* (eDP*) is an embedded version of the DisplayPort standard oriented towards applications such as notebook and All-In-One PCs. Like DisplayPort, embedded DisplayPort also consists of a Main Link, Auxiliary channel, and an optional Hot-Plug Detect signal.

### Integrated Audio

- HDMI and display port interfaces carry audio along with video.
- Processor supports two DMA controllers to output two High Definition audio streams on two digital ports simultaneously.
- Supports only the internal HDMI and DP CODECs.

### Table 4. Processor Supported Audio Formats over HDMI*and DisplayPort*

| Audio Formats | HDMI* | DisplayPort* |
|---|---|---|
| AC-3 Dolby* Digital | Yes | Yes |
| Dolby Digital Plus | Yes | Yes |
| DTS-HD* | Yes | Yes |
| LPCM, 192 kHz/24 bit, 8 Channel | Yes | Yes |
| Dolby TrueHD, DTS-HD Master Audio*<br>(Lossless Blu-Ray Disc* Audio Format) | Yes | Yes |

The processor will continue to support Silent stream. Silent stream is an integrated audio feature that enables short audio streams, such as system events to be heard over the HDMI and DisplayPort monitors. The processor supports silent streams over the HDMI and DisplayPort interfaces at 44.1 kHz, 48 kHz, 88.2 kHz, 96 kHz, 176.4 kHz, and 192 kHz sampling rates.

### Multiple Display Configurations

The following multiple display configuration modes are supported (with appropriate driver software):

- Single Display is a mode with one display port activated to display the output to one display device. If the external port is activated, it should always use the physical port B.
- Intel Display Clone is a mode with up to three display ports activated to drive the display content of same color depth setting but potentially different refresh rate and resolution settings to all the active display devices connected.
- Extended Desktop is a mode with up to three display ports activated to drive the content with potentially different color depth, refresh rate, and resolution settings on each of the active display devices connected.

The digital ports on the processor can be configured to support DisplayPort*/HDMI. The following table shows examples of valid three display configurations through the processor.

**Table 5. Multiple Display Configuration for Y-Processor Line**

| Display 1 | Display 2 | Display 3 | Maximum Resolution Display 1 | Maximum Resolution Display 2 | Maximum Resolution Display 3 |
|---|---|---|---|---|---|
| HDMI | HDMI | eDP | 4096x2304 @ 24 Hz | | 3200x2000 @ 60 Hz |
| DP | DP | eDP | 3200x2000 @ 60 Hz | | 3200x2000 @ 60 Hz |
| HDMI | DP | eDP | 4096x2304 @ 24 Hz | 3200x2000 @ 60 Hz | 3200x2000 @ 60 Hz |
| DP | eDP | N/A | *3840x2160 @ 60 Hz | *2560x1600 @ 60 Hz | N/A |

*Notes:* 1. DP and eDP resolutions in this table are supported for 4 lanes with link data rate HBR2 at 24 bits per pixel (bpp) and single stream mode of operation.

2. Dp and eDP resolutions of 3200x2000 @ 60 Hz require additional 100 mW cooling for the platform.

3. * To support maximum display resolution of 3840 x 2160 @ 60 Hz on DP or eDP, extra cooling is required and only two displays can be supported as shown in the table.

The following table shows the DisplayPort / embedded DisplayPort* resolutions supported for 1, 2, or 4 lanes depending on link data rate of RBR, HBR, HBR2.

**Table 6. DisplayPort and embedded DisplayPort* Resolutions for 1, 2, 4 Lanes – Link Data Rate of RBR, HBR, and HBR2 for Y-Processor Line**

| Link Data Rate | Lane Count | | |
|---|---|---|---|
| | 1 | 2 | 4 |
| RBR | 1064x600 | 1400x1050 | 2240x1400 |
| HBR | 1280x960 | 1920x1200 | 2560x1600 |
| HBR2 | 1920x1200 | 2880x1800 | 3200x2000 |

### High-bandwidth Digital Content Protection (HDCP)

HDCP is the technology for protecting high-definition content against unauthorized copy or unreceptive between a source (computer, digital set top boxes, and so on) and the sink (panels, monitor, and TVs). The processor supports HDCP 1.4 for content protection over wired displays (HDMI* and DisplayPort*).

The HDCP 1.4 keys are integrated into the processor and customers are not required to physically configure or handle the keys.

## 2.5 Platform Environmental Control Interface (PECI)

PECI is an Intel proprietary interface that provides a communication channel between Intel processors and external components, like Super I/O (SIO) and Embedded Controllers (EC), to provide processor temperature, Turbo, Configurable TDP, and memory throttling control mechanisms and many other services. PECI is used for platform thermal management and real time control and configuration of processor features and performance.

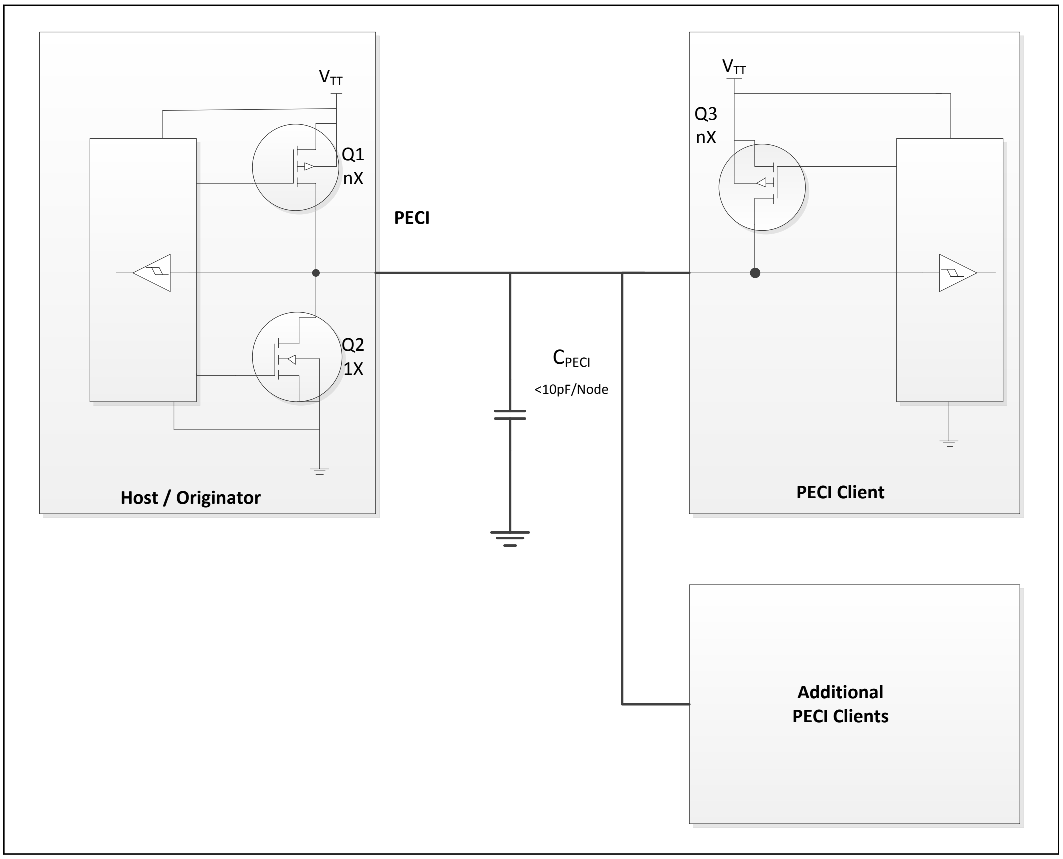
### 2.5.1 PECI Bus Architecture

The PECI architecture is based on a 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.

The following figure demonstrates PECI design and connectivity. While the host/originator can be a third party PECI host, one of the PECI clients is a processor PECI device.

## Figure 6. PECI Host-Clients Connection Example



# 3.0 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) for IA-32, Intel® 64 and Intel® Architecture (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) extends Intel® VT-x by adding hardware assisted support to improve I/O device virtualization performance.

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 Intel VT documents can be referenced at:

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

https://sharedspaces.intel.com/sites/PCDC/SitePages/Ingredients/ingredient.aspx?ing=VT

### 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 an improved 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 off-the-shelf operating systems and applications can be run 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.

### Intel® VT-x Features

The processor supports the following Intel VT-x features:

- Extended Page Table (EPT) Accessed and Dirty Bits
  - EPT A/D bits enabled VMMs to efficiently implement memory management and page classification algorithms to optimize VM memory operations, such as de-fragmentation, paging, live migration, and check-pointing. Without hardware support for EPT A/D bits, VMMs may need to emulate A/D bits by marking EPT paging-structures as not-present or read-only, and incur the overhead of EPT page-fault VM exits and associated software processing.
- Extended Page Table Pointer (EPTP) switching
  - EPTP switching is a specific VM function. EPTP switching allows guest software (in VMX non-root operation, supported by EPT) to request a different EPT paging-structure hierarchy. This is a feature by which software in VMX non-root operation can request a change of EPTP without a VM exit. Software can choose among a set of potential EPTP values determined in advance by software in VMX root operation.
- Pause loop exiting
  - Support VMM schedulers seeking to determine when a virtual processor of a multiprocessor virtual machine is not performing useful work. This situation may occur when not all virtual processors of the virtual machine are currently scheduled and when the virtual processor in question is in a loop involving the PAUSE instruction. The new feature allows detection of such loops and is thus called PAUSE-loop exiting.

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 the guest operating system 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 operating system 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) guarantees.

- Descriptor-Table Exiting
  - Descriptor-table exiting allows a VMM to protect a guest operating system from an 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.

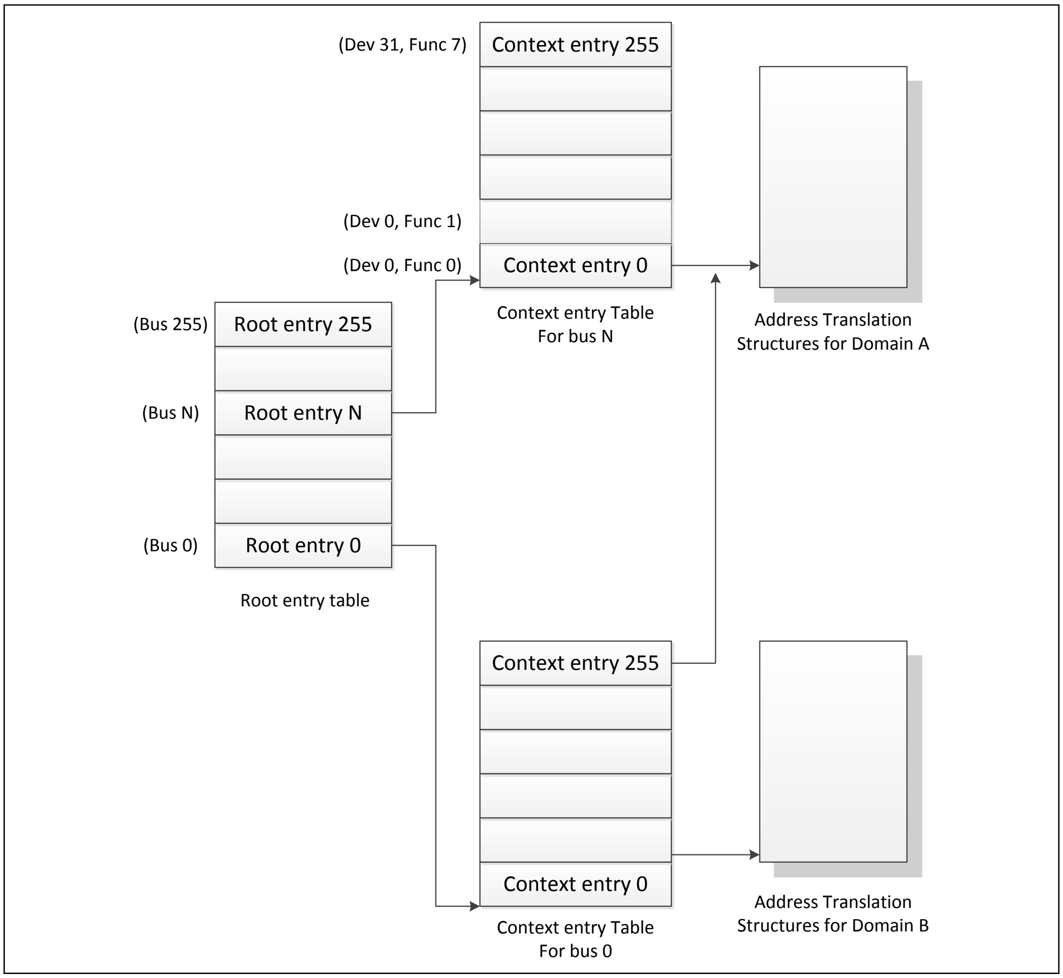
### Intel® VT-d Objectives

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. Intel VT-d provides accelerated I/O performance for a virtualized platform and provides software with the following capabilities:

- I/O device assignment and security: for flexibly assigning I/O devices to VMs and extending the protection and isolation properties of VMs for I/O operations.
- DMA remapping: for supporting independent address translations for Direct Memory Accesses (DMA) from devices.
- Interrupt remapping: for supporting isolation and routing of interrupts from devices and external interrupt controllers to appropriate VMs.
- Reliability: for recording and reporting to system software DMA and interrupt errors that may otherwise corrupt memory or impact VM isolation.

Intel VT-d accomplishes address translation by associating a transaction from a given I/O device to a translation table associated with the Guest to which the device is assigned. It does this by means of the data structure in the following illustration. This table creates an association between the device's PCI Express* Bus/Device/Function (B/D/F) number and the base address of a translation table. This data structure is populated by a VMM to map devices to translation tables in accordance with the device assignment restrictions above, and to include a multi-level translation table (VT-d Table) that contains Guest specific address translations.

## Figure 7. Device to Domain Mapping Structures



Intel VT-d functionality, often referred to as an Intel VT-d Engine, has typically been implemented at or near a PCI Express host bridge component of a computer system. This might be in a chipset component or in the PCI Express functionality of a processor with integrated I/O. When one such Intel VT-d engine receives a PCI Express transaction from a PCI Express bus, it uses the B/D/F number associated with the transaction to search for an Intel VT-d translation table. In doing so, it uses the B/D/F number to traverse the data structure shown in the above figure. If it finds a valid Intel VT-d table in this data structure, it uses that table to translate the address provided on the PCI Express bus. If it does not find a valid translation table for a given translation, this results in an Intel VT-d fault. If Intel VT-d translation is required, the Intel VT-d engine performs an N-level table walk.

For more information, refer to *Intel® Virtualization Technology for Directed I/O Architecture Specification* http://download.intel.com/technology/computing/vptech/Intel(r)_VT_for_Direct_IO.pdf

### Intel® VT-d Features

The processor supports the following Intel VT-d features:

- Memory controller and processor graphics comply with the Intel VT-d 1.2 Specification
- Two Intel VT-d DMA remap engines
  - iGFX DMA remap engine
  - Default DMA remap engine (covers all devices except iGFX)
- Support for root entry, context entry, and default context
- 39-bit guest physical address and host physical address widths
- Support for 4 KB, 2 MB, and 1 GB page sizes
- 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 Global, Domain specific, and Page specific 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
- Intel VT-d translation bypass address range is supported (Pass Through)

The processor supports the following added new Intel VT-d features:

- Intel VT-d superpage: support of Intel VT-d superpage (2 MB, 1 GB) for the default Intel VT-d engine and Intel VT-D IGD engine (iGFX DMA remap engine
- Support for LPSS device virtualization

*Note:* Intel VT-d Technology may not be available on all SKUs.

## 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.

The processor also offers additional enhancements to System Management Mode (SMM) architecture for enhanced security and performance. The processor provides new MSRs to:

- Enable a second SMM range
- Enable SMM code execution range checking
- Select whether SMM Save State is to be written to legacy SMRAM or to MSRs
- Determine if a thread is going to be delayed entering SMM
- Determine if a thread is blocked from entering SMM
- Targeted SMI, enable/disable threads from responding to SMIs both VLWs and IPI

For the above features, BIOS must test the associated capability bit before attempting to access any of the above registers.

For more information, refer to the Intel® Trusted Execution Technology Measured Launched Environment Programming Guide.

## 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* 8 and Microsoft Windows* 7 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 2.0

The Intel Turbo Boost Technology 2.0 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 2.0 feature is designed to increase performance of both multi-threaded and single-threaded workloads.

Compared with previous generation products, Intel Turbo Boost Technology 2.0 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 2.0 may not be available on all SKUs.

### Intel® Turbo Boost Technology 2.0 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 core current consumption.
- The estimated package prior and present power consumption.
- The package 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 within its TDP limit. Turbo processor frequencies are only active if the operating system is requesting the P0 state. For more information on P-states and C-states, see Power Management on page 40.

## 3.5 Intel® Advanced Vector Extensions 2.0 (Intel® AVX2)

Intel Advanced Vector Extensions 2.0 (Intel AVX2) is the latest expansion of the Intel instruction set. Intel AVX2 extends the Intel Advanced Vector Extensions (Intel AVX) with 256-bit integer instructions, floating-point fused multiply add (FMA) instructions, and gather operations. The 256-bit integer vectors benefit math, codec, image, and digital signal processing software. FMA improves performance in face detection, professional imaging, and high performance computing. Gather operations increase vectorization opportunities for many applications. In addition to the vector extensions, this generation of Intel processors adds new bit manipulation instructions useful in compression, encryption, and general purpose software.

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 Intel 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.

### 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.

### Intel® Secure Key

The processor supports Intel® Secure Key (formerly known as Digital Random Number Generator (DRNG)), a software visible random number generation mechanism supported by a high quality entropy source. This capability is available to programmers through the RDRAND instruction. The resultant random number generation capability is designed to comply with existing industry standards in this regard (ANSI X9.82 and NIST SP 800-90).

Some possible usages of the RDRAND instruction include cryptographic key generation as used in a variety of applications, including communication, digital signatures, secure storage, and so on.

The processor has a RDSEED instruction that enables system software and security vendors who need to seed or reseed a software PRNG.

The RDSEED instruction will be a companion to the RDRAND instruction. RDSEED, along with RDRAND, fills out Intel's standards compliant (such as NIST SP800-90 A, B, and C) Hardware-based Random Number Generator portfolio.

## 3.7 Intel® 64 Architecture x2APIC

The x2APIC architecture extends the xAPIC architecture that provides key mechanisms for interrupt delivery. This extension is primarily intended 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 memory mapped interface to a 4K-Byte 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, ((2^20) – 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 x2APIC mode. The Memory Mapped IO (MMIO) interface used by xAPIC is not supported in 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 x2APIC mode.
- The x2APIC architecture provides backward compatibility to the xAPIC architecture and forward extendible for future Intel platform innovations.

*Note:* Intel x2APIC Technology may not be available on all SKUs.

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

## 3.8 Power Aware Interrupt Routing (PAIR)

The processor includes enhanced power-performance technology that routes interrupts to threads or cores based on their sleep states. As an example, for energy savings, it routes the interrupt to the active cores without waking the deep idle cores. For performance, it routes the interrupt to the idle (C1) cores without interrupting the already heavily loaded cores. This enhancement is mostly beneficial for high-interrupt scenarios like Gigabit LAN, WLAN peripherals, and so on.

## 3.9 Execute Disable Bit

The Execute Disable Bit allows memory to be marked as executable when combined with a supporting operating system. If code attempts to run in non-executable memory, the processor raises an error to the operating system. This feature can prevent some classes of viruses or worms that exploit buffer overrun vulnerabilities and can thus help improve the overall security of the system. See the *Intel® 64 and IA-32 Architectures Software Developer's Manuals* for more detailed information.

## 3.10 Intel® Device Protection with Boot Guard

Intel® Device Protection with Boot Guard can help protect the platform boot integrity by preventing execution of unauthorized boot blocks. With Intel® Device Protection with Boot Guard, platform manufacturers can create boot policies such that invocation of an unauthorized (or untrusted) boot block will trigger the platform protection per the manufacturer's defined policy.

With verification based in the hardware, Intel® Device Protection with Boot Guard extends the trust boundary of the platform boot process down to the hardware level.

Intel® Device Protection with Boot Guard accomplishes this by:

- Providing hardware-based Static Root of Trust for Measurement (S-RTM) and the Root of Trust for Verification (RTV) using Intel architectural components.
- Providing architectural definition for platform manufacturer Boot Policy.
- Enforcing manufacture provided Boot Policy using Intel architectural components.

Benefits of this protection is that Intel® Device Protection with Boot Guard can help maintain platform integrity by preventing re-purposing of the manufacturer’s hardware to run an unauthorized software stack.

*Note:* Intel® Device Protection with Boot Guard technology availability may vary between the different SKUs.

## 3.11 Supervisor Mode Execution Protection (SMEP)

Supervisor Mode Execution Protection provides the next level of system protection by blocking malicious software attacks from user mode code when the system is running in the highest privilege level. This technology helps to protect from virus attacks and unwanted code from harming the system. For more information, refer to *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A* at: http://www.intel.com/Assets/PDF/manual/253668.pdf

## 3.12 Supervisor Mode Access Protection (SMAP)

Supervisor Mode Access Protection provides the next level of system protection by blocking a malicious user from tricking the operating system into branching off user data. This technology shuts down very popular attack vectors against operating systems . For more information, refer to the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A.*

## 3.13 Intel® Transactional Synchronization Extensions - New Instructions (Intel® TSX-NI)

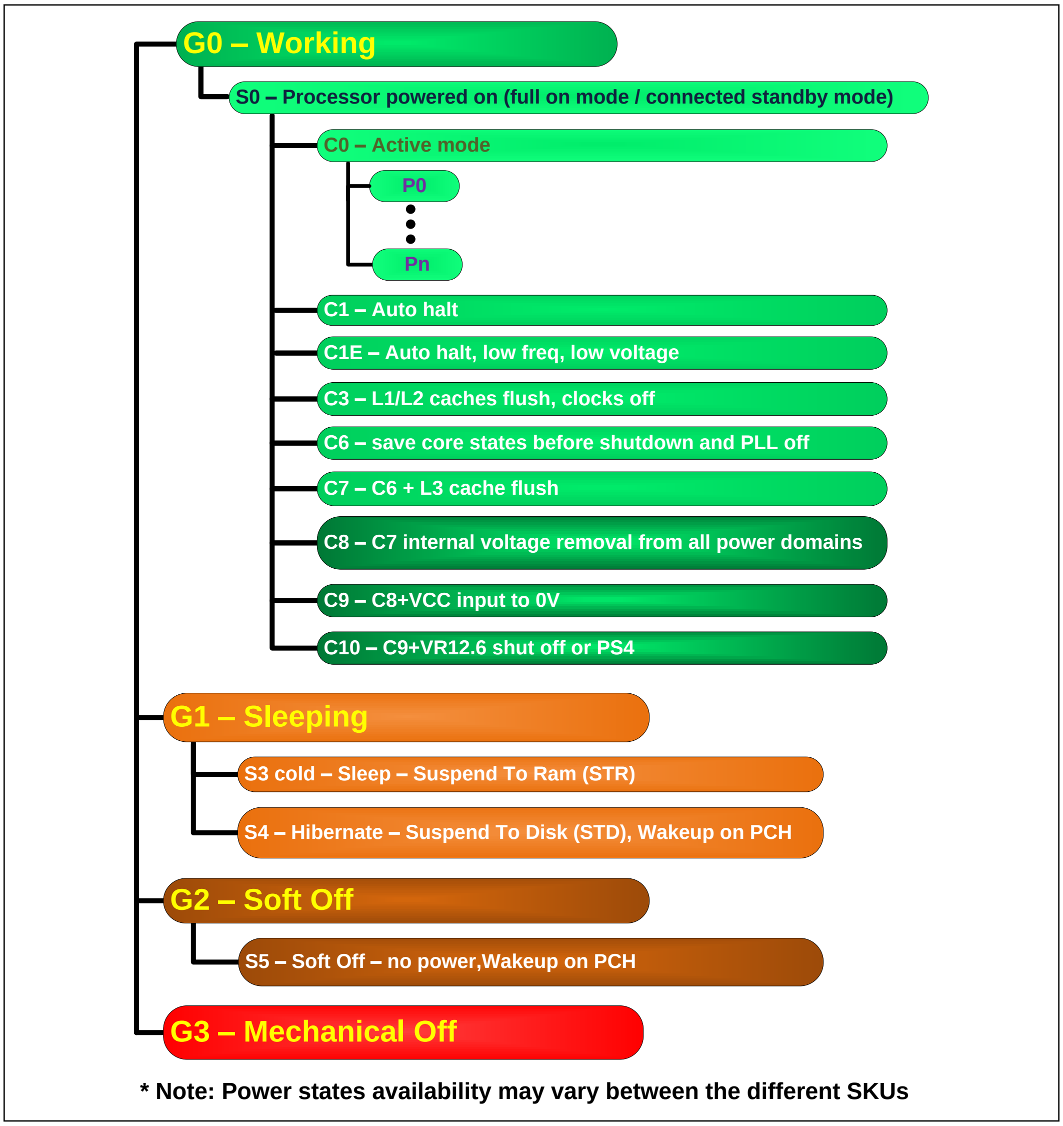
The processor supports Intel Transactional Synchronization Extensions - New Instructions (Intel TSX-NI). Intel TSX-NI provides a set of instruction extensions that allow programmers to specify regions of code for transactional synchronization. Programmers can use these extensions to achieve the performance of fine-grain locking while actually programming using coarse-grain locks. Details on Intel TSX-NI are in the *Intel® Architecture Instruction Set Extensions Programming Reference.*

# 4.0 Power Management

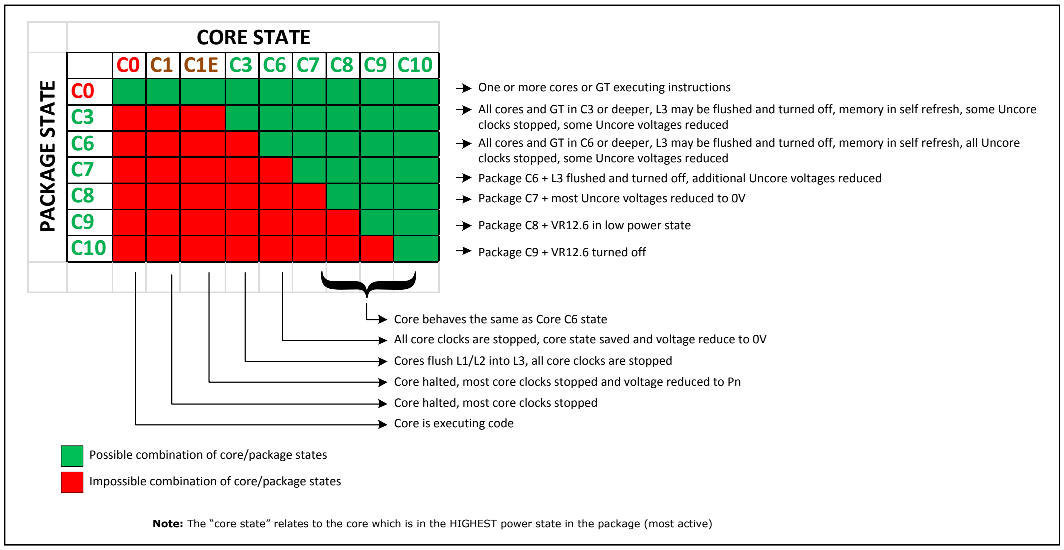
This chapter provides information on the following power management topics:

- Advanced Configuration and Power Interface (ACPI) States
- Processor Core
- Integrated Memory Controller (IMC)
- Processor Graphics Controller

**Figure 8. Processor Power States**


G0 – Working
S0 – Processor powered on (full on mode / connected standby mode)
C0 – Active mode
P0
Pn
C1 – Auto halt
C1E – Auto halt, low freq, low voltage
C3 – L1/L2 caches flush, clocks off
C6 – save core states before shutdown and PLL off
C7 – C6 + L3 cache flush
C8 – C7 internal voltage removal from all power domains
C9 – C8+VCC input to 0V
C10 – C9+VR12.6 shut off or PS4
G1 – Sleeping
S3 cold – Sleep – Suspend To Ram (STR)
S4 – Hibernate – Suspend To Disk (STD), Wakeup on PCH
G2 – Soft Off
S5 – Soft Off – no power,Wakeup on PCH
G3 – Mechanical Off
* Note: Power states availability may vary between the different SKUs

### Figure 9. Processor Package and Core C-States



| PACKAGE STATE \ CORE STATE | C0 | C1 | C1E | C3 | C6 | C7 | C8 | C9 | C10 |
|---|---|---|---|---|---|---|---|---|---|
| C0 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| C3 | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| C6 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| C7 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 |
| C8 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 |
| C9 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 |
| C10 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 |

- C0: One or more cores or GT executing instructions
- C3: All cores and GT in C3 or deeper, L3 may be flushed and turned off, memory in self refresh, some Uncore clocks stopped, some Uncore voltages reduced
- C6: All cores and GT in C6 or deeper, L3 may be flushed and turned off, memory in self refresh, all Uncore clocks stopped, some Uncore voltages reduced
- C7: Package C6 + L3 flushed and turned off, additional Uncore voltages reduced
- C8: Package C7 + most Uncore voltages reduced to 0V
- C9: Package C8 + VR12.6 in low power state
- C10: Package C9 + VR12.6 turned off

- C8, C9, C10: Core behaves the same as Core C6 state
- C6: All core clocks are stopped, core state saved and voltage reduce to 0V
- C3: Cores flush L1/L2 into L3, all core clocks are stopped
- C1E: Core halted, most core clocks stopped and voltage reduced to Pn
- C1: Core halted, most core clocks stopped
- C0: Core is executing code

🟩 Possible combination of core/package states

🟥 Impossible combination of core/package states

**Note:** The "core state" relates to the core which is in the HIGHEST power state in the package (most active)

## 4.1 Advanced Configuration and Power Interface (ACPI) States Supported

This section describes the ACPI states supported by the processor.

### Table 7. System States

| State | Description |
|---|---|
| G0/S0 | Full On Mode, Display On. |
| G0/S0 | Connected Standby Mode, Display Off. |
| G1/S3-Cold | Suspend-to-RAM (STR). Context saved to memory (S3-Hot state is not supported by the processor). |
| G1/S4 | Suspend-to-Disk (STD). All power lost (except wakeup on PCH). |
| G2/S5 | Soft off. All power lost (except wakeup on PCH). Total reboot. |
| G3 | Mechanical off. All power removed from system. |

### Table 8. Processor Core / Package State Support

| State | Description |
|---|---|
| C0 | Active mode, processor executing code. |
| C1 | AutoHALT state. |
| C1E | AutoHALT state with lowest frequency and voltage operating point. |
| C3 | Execution cores in C3 state flush their L1 instruction cache, L1 data cache, and L2 cache to the L3 shared cache. Clocks are shut off to each core. |
| C6 | Execution cores in this state save their architectural state before removing core voltage. |

*continued...*

| State | Description |
|---|---|
| C7 | Execution cores in this state behave similarly to the C6 state. If all execution cores request C7 state, L3 cache ways are flushed until it is cleared. If the entire L3 cache is flushed, voltage will be removed from the L3 cache. Power removal to SA, Cores and L3 will reduce power consumption. |
| C8 | C7 state plus voltage is removed from all power domains after required state is saved. PLL is powered down. |
| C9 | C8 state plus processor $V_{CC}$ input voltage at 0 V. |
| C10 | C9 state plus VR12.6 is set to low-power state, near shut off. |

**Table 9. Integrated Memory Controller States**

| State | Description |
|---|---|
| Power up | CKE asserted. Active mode. |
| Pre-charge Power-down | CKE de-asserted (not self-refresh) with all banks closed. |
| Active Power-down | CKE de-asserted (not self-refresh) with minimum one bank active. |
| Self-Refresh | CKE de-asserted using device self-refresh. |

**Table 10. G, S, and C Interface State Combinations**

| Global (G) State | Sleep (S) State | Processor Package (C) State | Processor State | System Clocks | Description |
|---|---|---|---|---|---|
| G0 | S0 | C0 | Full On | On | Full On |
| G0 | S0 | C1/C1E | Auto-Halt | On | Auto-Halt |
| G0 | S0 | C3 | Deep Sleep | On | Deep Sleep |
| G0 | S0 | C6/C7 | Deep Power-down | On | Deep Power-down |
| G0 | S0 | C8/C9/C10 | | On | Deeper Power-down |
| G1 | S3 | Power off | | Off, except RTC | Suspend to RAM |
| G1 | S4 | Power off | | Off, except RTC | Suspend to Disk |
| G2 | S5 | Power off | | Off, except RTC | Soft Off |
| G3 | NA | Power off | | Power off | Hard off |

## 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, deeper power C-states have longer entry and exit latencies.

### 4.2.1 Enhanced Intel® SpeedStep® Technology Key Features

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

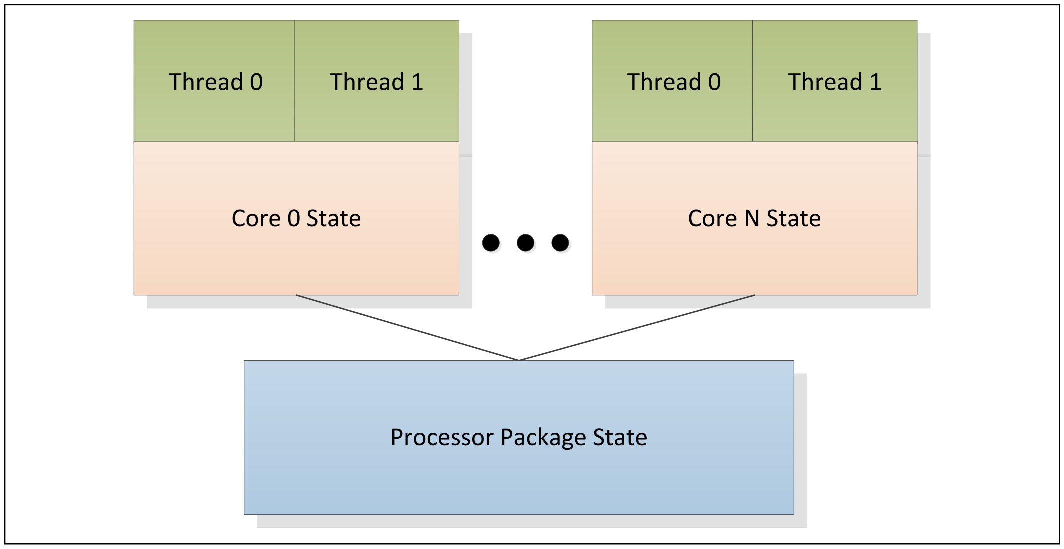
- Multiple frequency and voltage points for optimal performance and power efficiency. These operating points are known as P-states.
- Frequency selection is software controlled by writing to processor MSRs. The voltage is optimized based on the selected frequency and the number of active processor cores.
  - Once the voltage is established, the PLL locks on to the target frequency.
  - All active processor cores share the same frequency and voltage. In a multi-core processor, the highest frequency P-state requested among 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 Hyper-Threading Technology is enabled.

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

**Figure 10. Idle Power Management Breakdown of the Processor Cores**



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.

### 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.

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 do not cause an I/O redirection to MWAIT(Cx) like request. The reads fall through like a normal I/O instruction.

*Note:* When P_LVLx I/O instructions are used, MWAIT sub-states cannot be defined. The MWAIT sub-state 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-State Rules

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 state while Thread 1 requests C3 state, resulting in a core C1E state). See the *G, S, and C Interface State Combinations* table.
- 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/Timed MWAIT instruction
  - The deadline corresponding to the Timed MWAIT instruction expires
- An interrupt directed toward a single thread wakes only that thread.
- If any thread in a core is in active (in C0 state), the core's C-state will resolve to C0 state.
- Any interrupt coming into the processor package may wake any core.
- A system reset re-initializes all processor cores.

#### Core C0 State

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

### 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 Architectures Software Developer's Manual* 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 state, see Package C-States on page 46.

### 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.

### 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 state, 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.

### Core C7-C10 States

Individual threads of a core can enter the C7, C8, C9, or C10 state by initiating a P_LVL4, P_LVL5, P_LVL6, P_LVL7 I/O read (respectively) to the P_BLK or by an MWAIT(C7/C8/C9/C10) instruction. The core C7–C10 state exhibits the same behavior as the core C6 state.

### C-State Auto-Demotion

In general, deeper C-states, such as C6 or C7 state, 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 battery life and idle power. To increase residency and improve battery life and idle power in deeper C-states, the processor supports C-state auto-demotion.

There are two C-state auto-demotion options:

- C7/C6 to C3 state
- C7/C6/C3 To C1 state

The decision to demote a core from C6/C7 to C3 or C3/C6/C7 to C1 state is based on each core's immediate residency history and interrupt rate . If the interrupt rate experienced on a core is high and the residence in a deep C-state between such interrupts is low, the core can be demoted to a C3 or C1 state. A higher interrupt pattern is required to demote a core to C1 state as compared to C3 state.

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, C6, C7, C8, C9, and C10 power states.The following is a summary of the general rules for package C-state entry. These apply to all package C-states, 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 state before entering any other C-state.
    - Entry into a package C-state may be subject to auto-demotion – that is, the processor may keep the package in a deeper package C-state than requested by the operating system if the processor determines, using heuristics, that the deeper C-state results in better power/performance.

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 state.
    - If the break event is masked, the processor attempts to re-enter its previous package state.
- 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 C-state, 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.

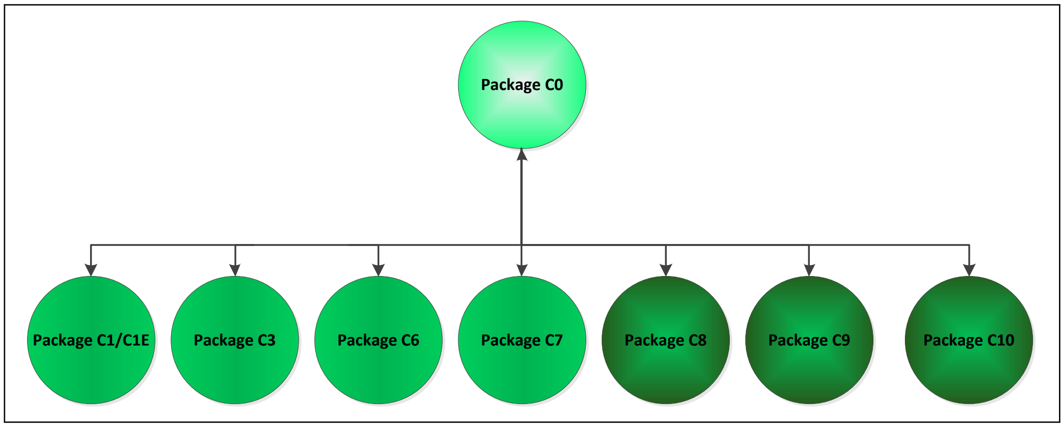
The following table shows package C-state resolution for a dual-core processor. The following figure summarizes package C-state transitions.

## Table 11. Coordination of Core Power States at the Package Level

| Package C-State | | Core 1 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **C0** | **C1** | **C3** | **C6** | **C7** | **C8** | **C9** | **C10** |
| **Core 0** | **C0** | C0 | C0 | C0 | C0 | C0 | C0 | C0 | C0 |
| | **C1** | C0 | C1[1] | C1[1] | C1[1] | C1[1] | C1[1] | C1[1] | C1[1] |
| | **C3** | C0 | C1[1] | C3 | C3 | C3 | C3 | C3 | C3 |
| | **C6** | C0 | C1[1] | C3 | C6 | C6 | C6 | C6 | C6 |
| | **C7** | C0 | C1[1] | C3 | C6 | C7 | C7 | C7 | C7 |
| | **C8** | C0 | C1[1] | C3 | C6 | C7 | C8 | C8 | C8 |
| | **C9** | C0 | C1[1] | C3 | C6 | C7 | C8 | C9 | C9 |
| | **C10** | C0 | C1[1] | C3 | C6 | C7 | C8 | C9 | C10 |

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

## Figure 11. Package C-State Entry and Exit



### Package C0 State

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 state.

### Package C1/C1E State

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 deeper 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 deeper than C1/C1E state; however, the package low-power state is limited to C1/C1E using the PMG_CST_CONFIG_CONTROL MSR.
- All cores have requested C1 state 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 state.

### Package C2 State

Package C2 state is an internal processor state that cannot be explicitly requested by software. A processor enters Package C2 state when:

- All cores and graphics have requested a C3 or deeper power state; however, constraints (LTR, programmed timer events in the near future, and so on) prevent entry to any state deeper than C 2 state. Or,
- All cores and graphics are in the C3 or deeper power states, and a memory access request is received. Upon completion of all outstanding memory requests, the processor transitions back into a deeper package C-state.

### 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 state or deeper power state and the processor has been granted permission by the platform.
- The platform has not granted a request to a package C6/C7 or deeper state, however, has allowed a package C6 state.

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

### 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 deeper power state and the processor has been granted permission by the platform.
- The platform has not granted a package C7 state or deeper request; however, has allowed a package C6 state.
- If the cores are requesting C7 state, but the platform is limiting to a package C6 state, the last level cache in this case can be flushed.

In package C6 state all cores have saved their architectural state and have had their core voltages reduced to zero volts. It is possible the L3 shared cache is flushed and turned off in package C6 state. If at least one core is requesting C6 state, the L3 cache will not be flushed.

### Package C7 State

The processor enters the package C7 low-power state when all cores are in the C7 state. In package C7, the processor will take action to remove power from portions of the system agent.

Core break events are handled the same way as in package C3 or C6 state.

### Package C8 State

The processor enters C8 states when the core with the highest state is C8.

The package C8 state is similar to package C7 state; however, in addition, all internally generated voltage rails are turned off and the input $V_{CC}$ is reduced to 1.15 V to 1.3 V.

### Package C9 State

The processor enters package C9 states when the core with the highest state is C9.

The package C9 state is similar to package C8 state; in addition, the input $V_{CC}$ is changed to 0 V.

### Package C10 State

The processor enters C10 states when the core with the highest state is C10.

The package C10 state is similar to the package C9 state; in addition, the VR12.6 is in PS4 low-power state, which is near to shut off of the VR12.6.

### Dynamic L3 Cache Sizing

When all cores request C7 or deeper C-state, internal heuristics is dynamically flushes the L3 cache. Once the cores enter a deep C-state, depending on their MWAIT substate request, the L3 cache is either gradually flushed N-ways at a time or flushed all at once. Upon the cores exiting to C0, the L3 cache is gradually expanded based on internal heuristics.

## 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 in which it is not connected to any actual memory devices 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 determined that the rows are not populated. This is due to the fact that when CKE is tri-stated with DRAMs present, the DRAMs are not ensured to maintain data integrity. CKE tri-state should be enabled by BIOS where appropriate, since at reset all rows must be assumed to be populated.

CKE tristate 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 memory interface.The processor drives four CKE pins, one per rank.

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 to the selected mode and the DDR type used. For more information, refer to the IDD table in the DDR specification.

The processor supports four different types of power-down modes in package C0. The different power-down modes can be enabled through configuring "PM_PDWN_config_0_0_0_MCHBAR". The type of CKE power-down can be configured through PDWN_mode (bits 15:12) and the idle timer can be configured through PDWN_idle_counter (bits 11:0). The different power-down modes supported are:

- **No power-down** (CKE disable)
- **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 defined by tXP – small number of cycles. For this mode, DRAM DLL must be on.
- **PPD/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. For this mode, DRAM DLL must be off.
- **Pre-charged power-down (PPD):** This mode is entered if all banks in DDR are pre-charged 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. The difference from APD mode is that when waking-up all page-buffers are empty.) The LPDDR does not have a DLL. As a result, the power savings are as good as PPD/DLL-off, but will have lower exit latency and higher performance.

The CKE is determined per rank, whenever 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 arrives 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 IMC can find many opportunities to power down ranks, even while running memory intensive applications; the savings are significant (may be 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 trade-offs 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 which tries to minimize power-consumption, try using the deepest power-down mode possible – PPD/DLL-off with a low idle timer value
- In high-performance systems with dense packaging (that is, tricky thermal design) the power-down mode should be considered in order to reduce the heating and avoid DDR throttling caused by the heating.

The default value that BIOS configures in "PM_PDWN_config_0_0_0_MCHBAR" is 6080h – that is, PPD/DLL-off mode with idle timer of 80h, or 128 DCLKs. This is a balanced setting with deep power-down mode and moderate idle timer value.

The idle timer expiration count defines the # of DCKLs that a rank is idle that causes entry to the selected powermode. As this timer is set to a shorter time, the IMC will have more opportunities to put DDR in power-down. There is no BIOS hook to set this register. Customers choosing to change the value of this register can do it by changing it in the BIOS. For experiments, this register can be modified in real time if BIOS does not lock the IMC registers.

### 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 DDR3L/DDR3L-RS 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 power-up. 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

During S0 idle state, system memory may be conditionally placed into self-refresh state when the processor is in package C3 or deeper power state. Refer to Intel® Rapid Memory Power Management (Intel® RMPM) for more details on conditional self-refresh with Intel HD Graphics enabled.

When entering the S3 – Suspend-to-RAM (STR) state or S0 conditional self-refresh, the processor core flushes pending cycles and then enters SDRAM ranks that are not used by Intel graphics memory into self-refresh. The CKE signals remain LOW so the SDRAM devices perform self-refresh.

The target behavior is to enter self-refresh for package C3 or deeper power states as long as there are no memory requests to service. The target usage is shown in the following table.

**Table 12. Targeted Memory State Conditions**

| Mode | Memory State with Processor Graphics | Memory State with External Graphics |
|---|---|---|
| C0, C1, C1E | Dynamic memory rank power-down based on idle conditions. | Dynamic memory rank power-down based on idle conditions. |
| C3, C6, C7 | If the processor graphics engine is idle and there are no pending display requests, then enter self-refresh. Otherwise, use dynamic memory rank power-down based on idle conditions. | If there are no memory requests, then enter self-refresh. Otherwise, use dynamic memory rank power-down based on idle conditions. |
| S3 | Self-Refresh Mode | Self-Refresh Mode |
| S4 | Memory power-down (contents lost) | Memory power-down (contents lost) |

#### 4.3.2.3 Dynamic Power-Down

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 power-down (CKE de-assertion with open pages) or pre-charge power-down (CKE de-assertion with all pages closed). Pre-charge 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, CKE, ODE, and CS signals are controlled per DIMM rank and will be powered down for unused ranks.

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).

### 4.3.3 DDR Electrical Power Gating (EPG)

The DDR I/O of the processor supports Electrical Power Gating (DDR-EPG) while the processor is at C3 or deeper power state.

In C3 or deeper power state, the processor internally gates $V_{DDQ}$ for the majority of the logic to reduce idle power while keeping all critical DDR pins such as CKE and VREF in the appropriate state.

In C7 or deeper power state, the processor internally gates $Vcc_{ST}$ for all non-critical state to reduce idle power.

In S3 or C-state transitions, the DDR does not go through training mode and will restore the previous training information.

## 4.4 Graphics Power Management

### 4.4.1 Intel® Rapid Memory Power Management (Intel® RMPM)

Intel Rapid Memory Power Management (Intel RMPM) conditionally places memory into self-refresh when the processor is in package C3 or deeper power state to allow the system to remain in the lower power states longer for memory not reserved for graphics memory. Intel RMPM functionality depends on graphics/display state (relevant only when processor graphics is being used), as well as memory traffic patterns generated by other connected I/O devices.

### 4.4.2 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. RC6 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 processor graphics will program the graphics render engine internal power rail into a low voltage state.

### 4.4.3 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. Intel 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.

### 4.4.4 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 guaranteed 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 try to place the graphics engine in the most energy efficient P-state.

### 4.4.5 Intel® Display Power Saving Technology (Intel® DPST)

The Intel DPST technique achieves backlight power savings while maintaining a good visual experience. This is accomplished by adaptively enhancing the displayed image while decreasing the backlight brightness simultaneously. The goal of this technique is to provide equivalent end-user-perceived image quality at a decreased backlight power level.

1. The original (input) image produced by the operating system or application is analyzed by the Intel DPST subsystem. An interrupt to Intel DPST software is generated whenever a meaningful change in the image attributes is detected. (A meaningful change is when the Intel DPST software algorithm determines that enough brightness, contrast, or color change has occurred to the displaying images that the image enhancement and backlight control needs to be altered.)
2. Intel DPST subsystem applies an image-specific enhancement to increase image contrast, brightness, and other attributes.

3. A corresponding decrease to the backlight brightness is applied simultaneously to produce an image with similar user-perceived quality (such as brightness) as the original image.

Intel DPST 6.0 has improved the software algorithms and has minor hardware changes to better handle backlight phase-in and ensures the documented and validated method to interrupt hardware phase-in.

### 4.4.6 Intel® Automatic Display Brightness

The Intel Automatic Display Brightness feature dynamically adjusts the backlight brightness based upon the current ambient light environment. This feature requires an additional sensor to be on the panel front. The sensor receives the changing ambient light conditions and sends the interrupts to the Intel Graphics driver. As per the change in Lux, (current ambient light illuminance), the new backlight setting can be adjusted through BLC. The converse applies for a brightly lit environment. Intel Automatic Display Brightness increases the backlight setting.

### 4.4.7 Intel® Seamless Display Refresh Rate Technology (Intel® SDRRS Technology)

When a Local Flat Panel (LFP) supports multiple refresh rates, the Intel Display Refresh Rate Switching power conservation feature can be enabled. The higher refresh rate will be used when plugged in with an AC power adaptor or when the end user has not selected/enabled this feature. The graphics software will automatically switch to a lower refresh rate for maximum battery life when the notebook is on battery power and when the user has selected/enabled this feature. There are two distinct implementations of Intel DRRS – static and seamless. The static Intel DRRS method uses a mode change to assign the new refresh rate. The seamless Intel DRRS method is able to accomplish the refresh rate assignment without a mode change and therefore does not experience some of the visual artifacts associated with the mode change (SetMode) method.

# 5.0 Thermal Management

The thermal solution provides both component-level and system-level thermal management. To allow for the optimal operation and long-term reliability of Intel processor-based systems, the system/processor thermal solution should be designed so that the processor:

- Remains below the maximum junction temperature ($Tj_{Max}$) specification at the maximum thermal design power (TDP).
- Conforms to system constraints, such as system acoustics, system skin-temperatures, and exhaust-temperature requirements.

***Caution:*** Thermal specifications given in this chapter are on the component and package level and apply specifically to the processor. Operating the processor outside the specified limits may result in permanent damage to the processor and potentially other components in the system.

## 5.1 Thermal Considerations

The processor TDP is the maximum sustained power that should be used for design of the processor thermal solution. TDP is a power dissipation and junction temperature operating condition limit, specified in this document, that is validated during manufacturing for the base configuration when executing a near worst case commercially available workload as specified by Intel for the SKU segment. TDP may be exceeded for short periods of time or if running a "power virus" workload.

The processor integrates multiple processing and graphics cores and PCH on a single package.This may result in differences in the power distribution across the die and must be considered when designing the thermal solution.

Intel® Turbo Boost Technology 2.0 allows processor cores and processor graphics cores to run faster than the guaranteed frequency. It is invoked opportunistically and automatically as long as the processor is conforming to its temperature, power delivery, and current specification limits. When Intel Turbo Boost Technology 2.0 is enabled:

- Applications are expected to run closer to TDP more often as the processor will attempt to maximize performance by taking advantage of available TDP headroom in the processor package.
- The processor may exceed the TDP for short durations to use any available thermal capacitance within the thermal solution. The duration and time of such operation can be limited by platform runtime configurable registers within the processor.
- Thermal solutions and platform cooling that are designed to less than thermal design guidance may experience thermal and performance issues since more applications will tend to run at or near TDP for significant periods of time.

*Note:* Intel Turbo Boost Technology 2.0 availability may vary between the different SKUs.

## 5.2 Intel® Turbo Boost Technology 2.0 Power Monitoring

When operating in turbo mode, the processor monitors its own power and adjusts the turbo frequencies to maintain the average power within limits over a thermally significant time period. The processor calculates the package power that consists of the processor core power and graphics core power. In the event that a workload causes the power to exceed program power limits, the processor will protect itself using the Adaptive Thermal Monitor.

## 5.3 Intel® Turbo Boost Technology 2.0 Power Control

Illustration of Intel Turbo Boost Technology 2.0 power control is shown in the following sections and figures. Multiple controls operate simultaneously allowing for customization for multiple system thermal and power limitations. These controls allow for turbo optimizations within system constraints and are accessible using MSR, MMIO, or PECI interfaces

### 5.3.1 Package Power Control

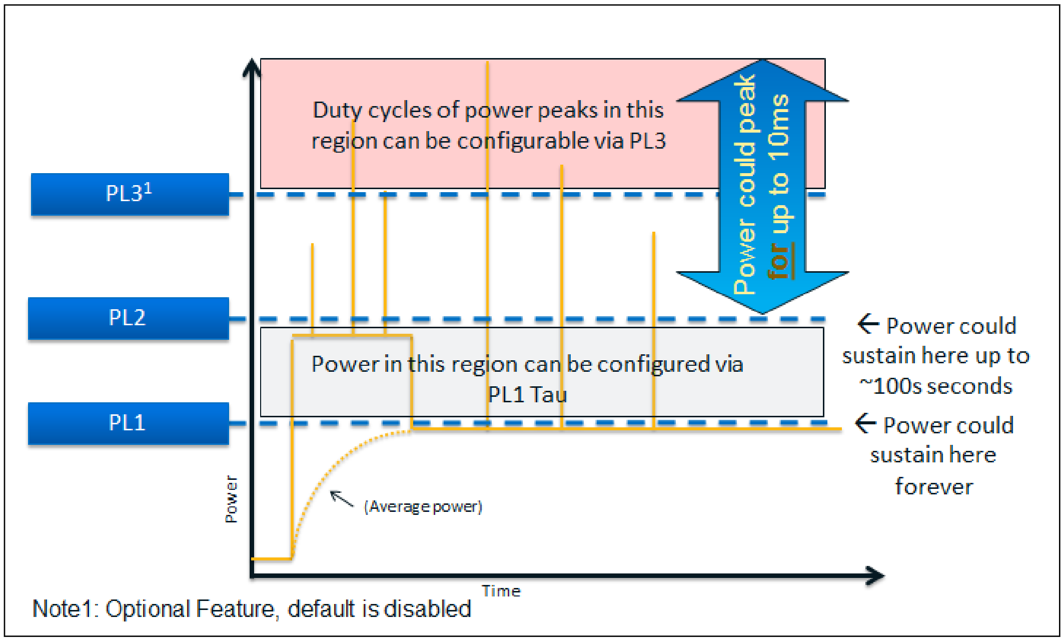
The package power control settings of PL1, PL2, and PL3 Tau allow the designer to configure Intel Turbo Boost Technology 2.0 to match the platform power delivery and package thermal solution limitations.

- Power Limit 1 (PL1): A threshold for average power that will not exceed - recommend to set to equal TDP power. PL1 should not be set higher than thermal solution cooling limits.
- Power Limit 2 (PL2): A threshold that if exceeded, the PL2 rapid power limiting algorithms will attempt to limit the spike above PL2.
- Power Limit 3 (PL3): A threshold that if exceeded, the PL3 rapid power limiting algorithms will attempt to limit the duty cycle of spikes above PL3 by reactively limiting frequency. This is an optional setting
- Turbo Time Parameter (Tau): An averaging constant used for PL1 exponential weighted moving average (EWMA) power calculation.

*Notes:*

- Implementation of Intel® Turbo Boost Technology 2.0 only requires configuring PL1, PL1 Tau and PL2.
- See the Turbo Implementation guide and BIOS Writers Guide (BWG) for additional details on use in your system (see related documents section).
- PL3 is disabled by default.

### Figure 12. Package Power Control


Duty cycles of power peaks in this region can be configurable via PL3
Power could peak for up to 10ms
PL3[1]
PL2
PL1
Power in this region can be configured via PL1 Tau
← Power could sustain here up to ~100s seconds
← Power could sustain here forever
(Average power)
Power
Time

Note1: Optional Feature, default is disabled

## 5.3.2 Turbo Time Parameter

Turbo Time Parameter is a mathematical parameter (units in seconds) that controls the Intel Turbo Boost Technology 2.0 algorithm using moving average of energy usage. During a maximum power turbo event of about 1.25 x TDP, the processor could sustain PL2 for up to approximately 1.5 times the Turbo Time Parameter. If the power value and/or Turbo Time Parameter is changed during runtime, it may take approximately 3 to 5 times the Turbo Time Parameter for the algorithm to settle at the new control limits. The time varies depending on the magnitude of the change and other factors. There is an individual Turbo Time Parameter associated with Package Power Control.

## 5.4 Configurable TDP (cTDP) and Low-Power Mode

Configurable TDP (cTDP) and Low-Power Mode (LPM) form a design vector where the processor's behavior and package TDP are dynamically adjusted to a desired system performance and power envelope. Configurable TDP and Low-Power Mode technologies offer opportunities to differentiate system design while running active workloads on select processor SKUs through scalability, configuration and adaptability. The scenarios or methods by which each technology is used are customizable but typically involve changes to PL1 and associated frequencies for the scenario with a resultant change in performance depending on system's usage. Either technology can be triggered by (but are not limited to) changes in OS power policies or hardware events such as docking a system, flipping a switch or pressing a button. cTDP and LPM are designed to be configured dynamically and do not require an operating system reboot.

*Note:* Configurable TDP and Low-Power Mode technologies are not battery life improvement technologies.

## 5.4.1 Configurable TDP

*Note:* Configurable TDP availability may vary between the different SKUs.

With cTDP, the processor is now capable of altering the maximum sustained power with an alternate IA core base frequency. Configurable TDP allows operation in situations where extra cooling is available or situations where a cooler and quieter mode of operation is desired. Configurable TDP can be enabled using Intel's DPTF driver or through HW/EC firmware. Enabling cTDP using the DPTF driver is recommended as Intel does not provide specific application or EC source code.

cTDP consists of three modes as shown in the following table.

### Table 13. Configurable TDP Modes

| Mode | Description |
|---|---|
| Base | The average power dissipation and junction temperature operating condition limit, specified in #unique_69/ unique_69_Connect_42_TABLE_EA4DAB3C1DAE42DFBDD0524DC42B151E, Table 14 on page 59 for the SKU Segment and Configuration, for which the processor is validated during manufacturing when executing an associated Intel-specified high-complexity workload at the processor IA core frequency corresponding to the configuration and SKU. |
| TDP-Up | The SKU-specific processor IA core frequency where manufacturing confirms logical functionality within the set of operating condition limits specified for the SKU segment and Configurable TDP-Up configuration in Table 5-2, Table 5-3 and Table 5-5. The Configurable TDP-Up Frequency and corresponding TDP is higher than the processor IA core Base Frequency and SKU Segment Base TDP. |
| TDP-Down | The processor IA core frequency where manufacturing confirms logical functionality within the set of operating condition limits specified for the SKU segment and Configurable TDP-Down configuration in Table 5-2, Table 5-3 and Table 5-5. The Configurable TDP-Down Frequency and corresponding TDP is lower than the processor IA core Base Frequency and SKU Segment Base TDP. |

In each mode, the Intel Turbo Boost Technology 2.0 power and frequency ranges are reprogrammed and the OS is given a new effective HFM operating point. The Intel DPTF driver assists in all these operations. The cTDP mode does not change the max per-core turbo frequency.

## 5.4.2 Low-Power Mode

Low-Power Mode (LPM) can provide cooler and quieter system operation. By combining several active power limiting techniques, the processor can consume less power while running at equivalent low frequencies. Active power is defined as processor power consumed while a workload is running and does not refer to the power consumed during idle modes of operation. LPM is only available using the Intel DPTF driver.

Through the DPTF driver, LPM can be configured to use each of the following methods to reduce active power:

- Restricting Intel Turbo Boost Power limits and IA core Turbo Boost availability
- Off-Lining core activity (Move processor traffic to a subset of cores)
- Placing an IA Core at LFM or LSF (Lowest Supported Frequency)
- Utilizing IA clock modulation
- Reducing number of active EUs to GT2 equivalent (Applicable for GT3 SKUs Only)

- LPM power as listed in the *TDP Specifications* table is defined at a point which IA cores working at MFM, GT = RPn and 1 core active

Off-lining core activity is the ability to dynamically scale a workload to a limited subset of cores in conjunction with a lower turbo power limit. It is one of the main vectors available to reduce active power. However, not all processor activity is ensured to be able to shift to a subset of cores. Shifting a workload to a limited subset of cores allows other cores to remain idle and save power. Therefore, when LPM is enabled, less power is consumed at equivalent frequencies.

Minimum Frequency Mode (MFM) of operation, which is the lowest supported frequency (LSF) at the LFM voltage, has been made available for use under LPM for further reduction in active power beyond LFM capability to enable cooler and quieter modes of operation.

## 5.5 Thermal and Power Specifications

The following notes apply to Table 14 on page 59 .

| Note | Definition |
|---|---|
| 1 | The TDP and Configurable TDP values are the average power dissipation in junction temperature operating condition limit, for the SKU Segment and Configuration, for which the processor is validated during manufacturing when executing an associated Intel-specified high-complexity workload at the processor IA core frequency corresponding to the configuration and SKU. |
| 2 | TDP workload may consist of a combination of processor-core intensive and graphics-core intensive applications. |
| 3 | The thermal solution needs to ensure that the processor temperature does not exceed the maximum junction temperature ($Tj_{MAX}$) limit, as measured by the DTS and the critical temperature bit. |
| 4 | The processor junction temperature is monitored by Digital Temperature Sensors (DTS). For DTS accuracy, refer to Digital Thermal Sensor Accuracy (Taccuracy) on page 62. |

**Table 14. Junction Temperature Specification**

| Segment | Symbol | Package Turbo Parameter | Min | Default | Max | Units | Notes |
|---|---|---|---|---|---|---|---|
| Y-Processor Line | $T_j$ | Junction temperature limit | 0 | — | 95 | ºC | 3, 4 |

## 5.6 Thermal Management Features

Occasionally the processor may operate in conditions that are near to its maximum operating temperature. This can be due to internal overheating or overheating within the platform. To protect the processor and the platform from thermal failure, several thermal management features exist to reduce package power consumption and thereby temperature in order to remain within normal operating limits. Furthermore, the processor supports several methods to reduce memory power.

### 5.6.1 Adaptive Thermal Monitor

The purpose of the Adaptive Thermal Monitor is to reduce processor core power consumption and temperature until it operates at or below its maximum operating temperature. Processor core power reduction is achieved by:

- Adjusting the operating frequency (using the core ratio multiplier) and voltage.

- Modulating (starting and stopping) the internal processor core clocks (duty cycle).

The Adaptive Thermal Monitor can be activated when the package temperature, monitored by any digital thermal sensor (DTS) meets or exceeds its maximum operating temperature. The maximum operating temperature implies either maximum junction temperature $Tj_{MAX}$, or $Tj_{MAX}$ minus TCC Activation offset.

Exceeding the maximum operating temperature activates the thermal control circuit (TCC), if enabled. When activated the thermal control circuit (TCC) causes both the processor core and graphics core to reduce frequency and voltage adaptively. The Adaptive Thermal Monitor will remain active as long as the package temperature exceeds its specified limit. Therefore, the Adaptive Thermal Monitor will continue to reduce the package frequency and voltage until the TCC is de-activated.

$Tj_{MAX}$ is factory calibrated and is not user configurable. The default value is software visible in the TEMPERATURE_TARGET (0x1A2) MSR, bits [23:16]. The TEMPERATURE_TARGET value stays the same when TCC Activation offset is enabled.

The Adaptive Thermal Monitor does not require any additional hardware, software drivers, or interrupt handling routines. It is not intended as a mechanism to maintain processor TDP. The system design should provide a thermal solution that can maintain TDP within its intended usage range.

*Note:* Adaptive Thermal Monitor protection is always enabled.

#### 5.6.1.1 Thermal Control Circuit (TCC) Activation Offset

TCC Activation Offset can be used to activate the Adaptive Thermal Monitor at temperatures lower than $Tj_{MAX}$. It is the preferred thermal protection mechanism for Intel Turbo Boost Technology 2.0 operation since ACPI passive throttling states will pull the processor out of turbo mode operation when triggered. An offset (in degrees Celsius) can be written to the TEMPERATURE_TARGET (0x1A2) MSR, bits [29:24]. This value will be subtracted from the value found in bits [23:16]. The default offset is 0 °C, TCC activation will occur at $Tj_{MAX}$. The offset should be set lower than any other protection such as ACPI _PSV trip points.

#### 5.6.1.2 Frequency / Voltage Control

Upon Adaptive Thermal Monitor activation, the processor core attempts to dynamically reduce processor core power by lowering the frequency and voltage operating point. The operating points are automatically calculated by the processor core itself and do not require the BIOS to program them as with previous generations of Intel processors. The processor core will scale the operating points such that:

- The voltage will be optimized according to the temperature, the core bus ratio, and number of cores in deep C-states.
- The core power and temperature are reduced while minimizing performance degradation.

Once the temperature has dropped below the maximum operating temperature, the operating frequency and voltage will transition back to the normal system operating point.

Once a target frequency/bus ratio is resolved, the processor core will transition to the new target automatically.

- On an upward operating point transition, the voltage transition precedes the frequency transition.
- On a downward transition, the frequency transition precedes the voltage transition.
- The processor continues to execute instructions. However, the processor will halt instruction execution for frequency transitions.

If a processor load-based Enhanced Intel SpeedStep Technology/P-state transition (through MSR write) is initiated while the Adaptive Thermal Monitor is active, there are two possible outcomes:

- If the P-state target frequency is higher than the processor core optimized target frequency, the P-state transition will be deferred until the thermal event has been completed.
- If the P-state target frequency is lower than the processor core optimized target frequency, the processor will transition to the P-state operating point.

### 5.6.1.3 Clock Modulation

If the frequency/voltage changes are unable to end an Adaptive Thermal Monitor event, the Adaptive Thermal Monitor will utilize clock modulation. Clock modulation is done by alternately turning the clocks off and on at a duty cycle (ratio between clock "on" time and total time) specific to the processor. The duty cycle is factory configured to 25% on and 75% off and cannot be modified. The period of the duty cycle is configured to 32 microseconds when the Adaptive Thermal Monitor is active. Cycle times are independent of processor frequency. A small amount of hysteresis has been included to prevent excessive clock modulation when the processor temperature is near its maximum operating temperature. Once the temperature has dropped below the maximum operating temperature, and the hysteresis timer has expired, the Adaptive Thermal Monitor goes inactive and clock modulation ceases. Clock modulation is automatically engaged as part of the Adaptive Thermal Monitor activation when the frequency/voltage targets are at their minimum settings. Processor performance will be decreased by the same amount as the duty cycle when clock modulation is active. Snooping and interrupt processing are performed in the normal manner while the Adaptive Thermal Monitor is active.

## 5.6.2 Digital Thermal Sensor

Each processor execution core has an on-die Digital Thermal Sensor (DTS) that detects the core's instantaneous temperature. The DTS is the preferred method of monitoring processor die temperature because:

- It is located near the hottest portions of the die.
- It can accurately track the die temperature and ensure that the Adaptive Thermal Monitor is not excessively activated.

Temperature values from the DTS can be retrieved through:

- A software interface using processor Model Specific Register (MSR).
- A processor hardware interface as described in Platform Environmental Control Interface (PECI) on page 27.

When temperature is retrieved by the processor MSR, it is the instantaneous temperature of the given core. When temperature is retrieved using PECI, it is the average of the highest DTS temperature in the package over a 256 ms time window.

Intel recommends using the PECI reported temperature for platform thermal control that benefits from averaging, such as fan speed control. The average DTS temperature may not be a good indicator of package Adaptive Thermal Monitor activation or rapid increases in temperature that triggers the Out of Specification status bit within the PACKAGE_THERM_STATUS MSR 1B1h and IA32_THERM_STATUS MSR 19Ch.

Code execution is halted in C1 or deeper C-states. Package temperature can still be monitored through PECI in lower C-states.

Unlike traditional thermal devices, the DTS outputs a temperature relative to the maximum supported operating temperature of the processor ($Tj_{MAX}$), regardless of TCC activation offset. It is the responsibility of software to convert the relative temperature to an absolute temperature. The absolute reference temperature is readable in the TEMPERATURE_TARGET MSR 1A2h. The temperature returned by the DTS is an implied negative integer indicating the relative offset from $Tj_{MAX}$. The DTS does not report temperatures greater than $Tj_{MAX}$. The DTS-relative temperature readout directly impacts the Adaptive Thermal Monitor trigger point. When a package DTS indicates that it has reached the TCC activation (a reading of 0h, except when the TCC activation offset is changed), the TCC will activate and indicate an Adaptive Thermal Monitor event. A TCC activation will lower both IA core and graphics core frequency, voltage, or both. Changes to the temperature can be detected using two programmable thresholds located in the processor thermal MSRs. These thresholds have the capability of generating interrupts using the core's local APIC. Refer to the *Intel® 64 and IA-32 Architectures Software Developer's Manual* for specific register and programming details.

#### 5.6.2.1 Digital Thermal Sensor Accuracy (Taccuracy)

The DTS is expected to work within ±5° C over the operating range

#### 5.6.2.2 Fan Speed Control with Digital Thermal Sensor

Digital Thermal Sensor based fan speed control ($T_{FAN}$) is a recommended feature to achieve optimal thermal performance. At the $T_{FAN}$ temperature, Intel recommends full cooling capability well before the DTS reading reaches $Tj_{MAX}$.

### 5.6.3 PROCHOT# Signal

PROCHOT# (processor hot) is asserted when the processor temperature has reached its maximum operating temperature ($Tj_{MAX}$). Only a single PROCHOT# pin exists at a package level. When any core arrives at the TCC activation point, the PROCHOT# signal will be asserted. PROCHOT# assertion policies are independent of Adaptive Thermal Monitor enabling.

#### 5.6.3.1 Bi-Directional PROCHOT#

By default, the PROCHOT# signal is set to bi-directional. However, it is recommended to configure the signal as an input only. When configured as an input or bi-directional signal, PROCHOT# can be used for thermally protecting other platform components in case the components overheat as well. When PROCHOT# is driven by an external device:

- The package will immediately transition to the lowest P-State (Pn) supported by the processor and graphics cores. This is contrary to the internally-generated Adaptive Thermal Monitor response.

- Clock modulation is not activated.

The processor package will remain at the lowest supported P-state until the system de-asserts PROCHOT#. The processor can be configured to generate an interrupt upon assertion and de-assertion of the PROCHOT# signal.

*Note:* When PROCHOT# is configured as a bi-directional signal and PROCHOT# is asserted by the processor, it is impossible for the processor to detect a system assertion of PROCHOT#. The system assertion will have to wait until the processor de-asserts PROCHOT# before PROCHOT# action can occur due to the system assertion. While the processor is hot and asserting PROCHOT#, the power is reduced; however, the reduction rate is slower than the system PROCHOT# response of < 100 us. The processor thermal control is staged in smaller increments over many milliseconds. This may cause several milliseconds of delay to a system assertion of PROCHOT# while the output function is asserted.

### 5.6.3.2 Voltage Regulator Protection using PROCHOT#

PROCHOT# may be used for thermal protection of voltage regulators (VR). System designers can create a circuit to monitor the VR temperature and assert PROCHOT# and, if enabled, activate the TCC when the temperature limit of the VR is reached. When PROCHOT# is configured as a bi-directional or input only signal, if the system assertion of PROCHOT# is recognized by the processor, it will result in an immediate transition to the lowest P-State (Pn) supported by the processor and graphics cores. Systems should still provide proper cooling for the VR and rely on bi-directional PROCHOT# only as a backup in case of system cooling failure. Overall, the system thermal design should allow the power delivery circuitry to operate within its temperature specification even while the processor is operating at its TDP.

### 5.6.3.3 Thermal Solution Design and PROCHOT# Behavior

With a properly designed and characterized thermal solution, it is anticipated that PROCHOT# will only be asserted for very short periods of time when running the most power intensive applications. The processor performance impact due to these brief periods of TCC activation is expected to be so minor that it would be immeasurable. However, an under-designed thermal solution that is not able to prevent excessive assertion of PROCHOT# in the anticipated ambient environment may:

- Cause a noticeable performance loss.
- Result in prolonged operation at or above the specified maximum junction temperature and affect the long-term reliability of the processor.
- May be incapable of cooling the processor even when the TCC is active continuously (in extreme situations).

### 5.6.3.4 Low-Power States and PROCHOT# Behavior

Depending on package power levels during package C-states, outbound PROCHOT# may de-assert while the processor is idle as power is removed from the signal. Upon wakeup, if the processor is still hot, the PROCHOT# will re-assert, although typically package idle state residency should resolve any thermal issues. The PECI interface is fully operational during all C-states and it is expected that the platform continues to manage processor core and package thermals even during idle states by regularly polling for thermal data over PECI.

#### 5.6.3.5 THERMTRIP# Signal

Regardless of enabling the automatic or on-demand modes, in the event of a catastrophic cooling failure, the package will automatically shut down when the silicon has reached an elevated temperature that risks physical damage to the product. At this point the THERMTRIP# signal will go active.

#### 5.6.3.6 Critical Temperature Detection

Critical Temperature detection is performed by monitoring the package temperature. This feature is intended for graceful shutdown before the THERMTRIP# is activated. However, the processor execution is not guaranteed between critical temperature and THERMTRIP#. If the Adaptive Thermal Monitor is triggered and the temperature remains high, a critical temperature status and sticky bit are latched in the PACKAGE_THERM_STATUS MSR 1B1h and the condition also generates a thermal interrupt, if enabled. For more details on the interrupt mechanism, refer to the *Intel® 64 and IA-32 Architectures Software Developer’s Manual*.

### 5.6.4 On-Demand Mode

The processor provides an auxiliary mechanism that allows system software to force the processor to reduce its power consumption using clock modulation. This mechanism is referred to as "On-Demand" mode and is distinct from Adaptive Thermal Monitor and bi-directional PROCHOT#. The processor platforms must not rely on software usage of this mechanism to limit the processor temperature. On-Demand Mode can be accomplished using processor MSR or chipset I/O emulation. On-Demand Mode may be used in conjunction with the Adaptive Thermal Monitor. However, if the system software tries to enable On-Demand mode at the same time the TCC is engaged, the factory configured duty cycle of the TCC will override the duty cycle selected by the On-Demand mode. If the I/O based and MSR-based On-Demand modes are in conflict, the duty cycle selected by the I/O emulation-based On-Demand mode will take precedence over the MSR-based On-Demand Mode.

#### 5.6.4.1 MSR Based On-Demand Mode

If Bit 4 of the IA32_CLOCK_MODULATION MSR is set to a 1, the processor will immediately reduce its power consumption using modulation of the internal core clock, independent of the processor temperature. The duty cycle of the clock modulation is programmable using bits [3:1] of the same IA32_CLOCK_MODULATION MSR. In this mode, the duty cycle can be programmed in either 12.5% or 6.25% increments (discoverable using CPUID). Thermal throttling using this method will modulate each processor core's clock independently.

#### 5.6.4.2 I/O Emulation-Based On-Demand Mode

I/O emulation-based clock modulation provides legacy support for operating system software that initiates clock modulation through I/O writes to ACPI defined processor clock control registers on the chipset (PROC_CNT). Thermal throttling using this method will modulate all processor cores simultaneously.

### 5.6.5 Intel® Memory Thermal Management

The processor provides thermal protection for system memory by throttling memory traffic when using either DIMM modules or a memory down implementation. Two levels of throttling are supported by the processor – either a warm threshold or hot threshold that is customizable through memory mapped I/O registers. Throttling based on the warm threshold should be an intermediate level of throttling. Throttling based on the hot threshold should be the most severe. The amount of throttling is dynamically controlled by the processor.

Memory temperature can be acquired through an on-board thermal sensor (TS-on-Board), retrieved by an embedded controller and reported to the processor through the PECI 3.0 interface. This methodology is known as PECI injected temperatures and is a method of Closed Loop Thermal Management (CLTM). CLTM requires the use of a physical thermal sensor. EXTTS# is another method of CLTM; however, it is only capable of reporting memory thermal status to the processor. EXTTS# consists of two GPIO pins on the PCH where the state of the pins is communicated internally to the processor.

When a physical thermal sensor is not available to report temperature, the processor supports Open Loop Thermal Management (OLTM) that estimates the power consumed per rank of the memory using the processor DRAM power meter. A per rank power is associated with the warm and hot thresholds that, when exceeded, may trigger memory thermal throttling.

### 5.6.6 Scenario Design Power (SDP)

Scenario Design Power (SDP) is a usage-based design specification, and provides an additional reference design point for power constrained platforms. SDP is a specified power level under a specific scenario workload, temperature, and frequency.

Intel recommends setting POWER_LIMIT_1 (PL1) to the system cooling capability (SDP level, or higher). While the SDP specification is characterized at Tj of 80 °C, the functional limit for the product remains at $Tj_{MAX}$. Customers may choose to have the processor invoke TCC Activation Throttling at 80 °C, but is not required.

The processors that have SDP specified can still exceed SDP under certain workloads, such as TDP workloads. TDP power dissipation is still possible with the intended usage models, and protection mechanisms to handle levels beyond cooling capabilities are recommended. Intel recommends using such thermal control mechanisms to manage situations where power may exceed the thermal design capability.

*Note:* cTDP-Down mode is required for Intel® Core™ processor products in order to achieve SDP.

*Note:* Although SDP is defined at 80 °C, the TCC activation temperature is 100 °C, and may be changed in BIOS to 80 °C.

# 6.0 Signal Description

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

| Notation | Signal Type |
|---|---|
| I | Input pin |
| O | Output pin |
| I/O | Bi-directional Input/Output pin |

The signal description also includes the type of buffer used for the particular signal (see the following table).

### Table 15. Signal Description Buffer Types

| Signal | Description |
|---|---|
| CMOS | CMOS buffers. 1.05V- tolerant |
| A | Analog reference or output. May be used as a threshold voltage or for buffer compensation |
| GTL | Gunning Transceiver Logic signaling technology |
| Ref | Voltage reference signal |
| Asynchronous [1] | Signal has no timing relationship with any reference clock. |
| 1. Qualifier for a buffer type. | |

## 6.1 System Memory Interface Signals

### Table 16. DDR3L / DDR3L-RS Memory Down Channel A and B Memory Signals

| Signal Name | Description | Direction / Buffer Type |
|---|---|---|
| SA_CK[0]/SA_CK#[0]<br>SB_CK[0]/SB_CK#[0] | **Clocks:** CK and its complement CK# signal make up a differential clock pair. The crossing of the positive edge of CK and the negative edge of its complement CK# are used to sample the command and control signals. | O |
| SA_MA[15:0],<br>SB_MA[15:0] | **Memory Address:** These signals are used to provide the multiplexed row and column address. | O |
| SA_BS[2:0], SB_BS[2;0] | **Bank Select:** Signals used to define which bank a command is being applied to. | O |
| SA_WE#, SB_WE# | **Write Enable:** These signals are used with RAS# and CAS# to define the command being entered. | O |
| SA_RAS#, SB_RAS# | **RAS:** These signals are used with CAS# and WE# to define the command being entered. | O |

continued...

| Signal Name | Description | Direction / Buffer Type |
|---|---|---|
| SA_CAS#, SB_CAS# | **CAS:** These signals are used with RAS# and WE# to define the command being entered. | O |
| SA_DQS[7:0]/<br>SA_DQS#[7:0]<br>SB_DQS[7:0]/<br>SB_DQS#[7:0] | **Data Strobes:** DQS and its complement DQS# signal make up a differential strobe pair. The data is captured at the crossing point of DQS and DQS# during read and write transactions. | I/O |
| SA_DQ[63:0],<br>SB_DQ[63:0] | **Data Bus:** Read and Write Input/Output data signals | I/O |
| SA_CS#[1:0],<br>SB_CS#[1:0] | **Chip Select :** These signals are used to select components during the active state. There is one Chip Select for each DRAM rank. | O |
| SA_CKE[1:0],<br>SB_CKE[1:0] | **Clock Enable:** These signals are used to initialize and power state components. There is one CKE for each DRAM rank. | O |
| SA_ODT[0], SB_ODT[0] | **On Die Termination:** Active Termination Control. | O |
| SM_DRAMRRST# | **DRAM RESET:** System Memory DRAM Device Reset. | O |
| VREF_DQ_A, VREF_DQ_B | **Data Reference Voltage:** Data Signal Reference Voltage. | O |
| VREF_CA | **Command/Address Reference Voltage:** Command and Address Signal Reference Voltage. | O |

## Table 17. LPDDR3 Memory Down Channel A and B Memory Signals

| Signal Name | Description | Direction / Buffer Type |
|---|---|---|
| SA_CK[1:0]/SA_CK#[1:0]<br>SB_CK[1:0]/SB_CK#[1:0] | **Clocks:** CK and its complement CK# signal make up a differential clock pair. The crossing of the positive edge of CK and the negative edge of its complement CK# are used to sample the command and control signals. | O |
| SA_CAA[9:0],<br>SA_CAB[9:0]<br>SB_CAA[9:0],<br>SB_CAB[9:0] | **Command Address:** These signals are used to provide the multiplexed command and address. | O |
| SA_DQS[7:0]/<br>SA_DQS#[7:0]<br>SB_DQS[7:0]/<br>SB_DQS#[7:0] | **Data Strobes:** DQS and its complement DQS# signal make up a differential strobe pair. The data is captured at the crossing point of DQS and DQS# during read and write transactions. | I/O |
| SA_DQ[63:0],<br>SB_DQ[63:0] | **Data Bus:** Read and Write Input/Output data signals. | I/O |
| SA_CS#[1:0],<br>SB_CS#[1:0] | **Chip Select :** These signals are used to select components during the active state. There is one Chip Select for each DRAM rank. | O |
| SA_CKE[3:0],<br>SB_CKE[3:0] | **Clock Enable:** These signals are used to initialize and power state components. There is one CKE for each DRAM rank. | O |
| SA_ODT[0], SB_ODT[0] | **On Die Termination:** Active Termination Control. | O |
| VREF_DQ_A, VREF_DQ_B | **Data Reference Voltage:** Data Signal Reference Voltage. | O |
| VREF_CA | **Command/Address Reference Voltage:** Command and Address Signal Reference Voltage. | O |

## 6.2 Memory Compensation and Miscellaneous Signals

### Table 18. LPDDR3 / DDR3L / DDR3L-RS Reference and Compensation Signals

| Signal Name | Description | Direction / Buffer Type |
|---|---|---|
| SM_RCOMP[2:0] | **System Memory Impedance Compensation:** | I |
| SM_PG_CNTL1 | **System Memory Power Gate Control:** This signal disables the platform memory VTT regulator in C8 and deeper and S3 states. | CMOS OUTPUT |

## 6.3 Reset and Miscellaneous Signals

### Table 19. Reset and Miscellaneous Signals

| Signal Name | Description | Direction / Buffer Type |
|---|---|---|
| CFG[19:0] | **Configuration Signals:** The CFG signals have a default value of '1' if not terminated on the board.<br>• **CFG[2:0]:** Reserved configuration lane. A test point may be placed on the board for these lanes.<br>• **CFG[3]: MSR Privacy Bit Feature**<br>— 1 = Debug capability is determined by IA32_Debug_Interface_MSR (C80h) bit[0] setting<br>— 0 = IA32_Debug_Interface_MSR (C80h) bit[0] default setting overridden<br>• **CFG[4]: eDP enable**<br>— 1 = Disabled<br>— 0 = Enabled<br>• **CFG[19:5]:** Reserved configuration lanes. A test point may be placed on the board for these lands. | I/O<br>GTL |
| CFG_RCOMP | Configuration resistance compensation. Use a 49.9 Ω ±1% resistor to ground. | — |
| FC_x | FC (Future Compatibility) signals are signals that are available for compatibility with other processors. A test point may be placed on the board for these lands. | |
| IST_TRIGGER | Signal is for IFDIM testing only. | I<br>CMOS |
| IVR_ERROR | Signal is for debug. If both THERMTRIP# and this signal are simultaneously asserted, the processor has encountered an unrecoverable power delivery fault and has engaged automatic shutdown as a result. | O<br>CMOS |
| RSVD<br>RSVD_TP | **RESERVED:** All signals that are RSVD must be left unconnected on the board. Intel recommends that all RSVD_TP signals have via test points. | No Connect<br>Test Point |
| TESTLO_x | TESTLO should be individually connected to $V_{SS}$ through a resistor. | |

## 6.4 embedded DisplayPort* (eDP*) Signals

### Table 20. embedded Display Port* Signals

| Signal Name | Description | Direction / Buffer Type |
|---|---|---|
| eDP_TXP[3:0]<br>eDP_TXN[3:0] | embedded DisplayPort Transmit Differential Pair | O<br>eDP |
| eDP_AUXP<br>eDP_AUXN | embedded DisplayPort Auxiliary Differential Pair | O<br>eDP |
| eDP_RCOMP | embedded DisplayPort Current Compensation | I/O<br>A |
| eDP_DISP_UTIL | Low voltage multipurpose DISP_UTIL pin on the processor for backlight modulation control of embedded panels and S3D device control for active shutter glasses. This pin will co-exist with functionality similar to existing BKLTCTL pin on the PCH. | O<br>Asynchronous CMOS |
| VCOMP_OUT | Internal processor power for eDP_RCOMP termination. | |

## 6.5 Display Interface Signals

### Table 21. Display Interface Signals

| Signal Name | Description | Direction / Buffer Type |
|---|---|---|
| DDIB_TXP[3:0]<br>DDIB_TXN[3:0] | Digital Display Interface Transmit Differential Pair | O<br>DP*/HDMI* |
| DDIC_TXP[3:0]<br>DDIC_TXN[3:0] | Digital Display Interface Transmit Differential Pair | O<br>DP*/HDMI* |

## 6.6 Phase Locked Loop (PLL) Signals

### Table 22. Phase Locked Loop (PLL) Signals

| Signal Name | Description | Direction / Buffer Type |
|---|---|---|
| BCLKP<br>BCLKN | Differential bus clock input to the processor | I<br>Diff Clk |
| DPLL_REF_CLKP<br>DPLL_REF_CLKN | Embedded Display Port PLL Differential Clock In: 135 MHz | I<br>Diff Clk |
| SSC_DPLL_REF_CLKP<br>SSC_ DPLL_REF_CLKN | Spread Spectrum Embedded DisplayPort PLL Differential Clock In: 135 MHz | I<br>Diff Clk |

## 6.7 Testability Signals

### Table 23. Testability Signals

| Signal Name | Description | Direction / Buffer Type |
|---|---|---|
| BPM#[7:0] | **Breakpoint and Performance Monitor Signals:** Outputs from the processor that indicate the status of breakpoints and programmable counters used for monitoring processor performance. | I/O<br>GTL |
| PRDY# | **Processor Ready:** This signal is a processor output used by debug tools to determine processor debug readiness. | O<br>GTL |
| PREQ# | **Processor Request:** This signal is used by debug tools to request debug operation of the processor. | I<br>GTL |
| PROC_TCK | **Test Clock:** This signal provides the clock input for the processor Test Bus (also known as the Test Access Port). This signal must be driven low or allowed to float during power on Reset. | I<br>GTL |
| PROC_TDI | **Processor Test Data In:** This signal transfers serial test data into the processor. This signal provides the serial input needed for JTAG specification support. | I<br>GTL |
| PROC_TDO | **Processor Test Data Out:** This signal transfers serial test data out of the processor. This signal provides the serial output needed for JTAG specification support. | O<br>Open Drain |
| PROC_TMS | **Processor Test Mode Select:** This is a JTAG specification supported signal used by debug tools. | I<br>GTL |
| PROC_TRST# | **Processor Test Reset:** This signal resets the Test Access Port (TAP) logic. This signal must be driven low during power on Reset. | I<br>GTL |

## 6.8 Error and Thermal Protection Signals

### Table 24. Error and Thermal Protection Signals

| Signal Name | Description | Direction / Buffer Type |
|---|---|---|
| CATERR# | **Catastrophic Error:** This signal indicates that the system has experienced a catastrophic error and cannot continue to operate. The processor will set this for non-recoverable machine check errors or other unrecoverable internal errors. CATERR# is used for signaling the following types of errors: Legacy MCERRs, CATERR# is asserted for 16 BCLKs. Legacy IERRs, CATERR# remains asserted until warm or cold reset. | O<br>GTL |
| PECI | **Platform Environment Control Interface:** A serial sideband interface to the processor, it is used primarily for thermal, power, and error management. | I/O<br>Asynchronous |
| PROCHOT# | **Processor Hot:** PROCHOT# goes active when the processor temperature monitoring sensor(s) detects that the processor has reached its maximum safe operating temperature. This indicates that the processor Thermal Control Circuit (TCC) has been activated, if enabled. This signal can also be driven to the processor to activate the TCC. | GTL Input<br>Open-Drain Output |
| THERMTRIP# | **Thermal Trip:** The processor protects itself from catastrophic overheating by use of an internal thermal sensor. This sensor is set well above the normal operating temperature to ensure that there are no false trips. The processor will stop all execution when the junction temperature exceeds approximately 130 °C. This is signaled to the system by the THERMTRIP# pin. | O<br>Asynchronous OD |

## 6.9 Power Sequencing Signals

### Table 25. Power Sequencing Signals

| Signal Name | Description | Direction / Buffer Type |
|---|---|---|
| PROCPWRGD | The processor requires this input signal to be a clean indication that the $V_{CC}$ and $V_{DDQ}$ power supplies are stable and within specifications. This requirement applies regardless of the S-state of the processor. 'Clean' implies that the signal will remain low (capable of sinking leakage current), without glitches, from the time that the power supplies are turned on until the supplies come within specification. The signal must then transition monotonically to a high state. | I<br>Asynchronous CMOS |
| VCCST_PWRGD | The processor requires this input signal to be a clean indication that the $V_{CCST}$ and $V_{DDQ}$ power supplies are stable and within specifications. This single must have a valid level during both S0 and S3 power states. 'Clean' implies that the signal will remain low (capable of sinking leakage current), without glitches, from the time that the power supplies are turned on until the supplies come within specification. The signal must then transition monotonically to a high state." | I<br>Asynchronous CMOS |
| PROC_DETECT# | **(Processor Detect):** This signal is pulled down directly (0 Ohms) on the processor package to ground. There is no connection to the processor silicon for this signal. System board designers may use this signal to determine if the processor is present. | — |

## 6.10 Processor Power Signals

### Table 26. Processor Power Signals

| Signal Name | Description | Direction / Buffer Type |
|---|---|---|
| VCC | Processor main power rail. | Ref |
| VDDQ | Processor I/O supply voltage for DDR3L/DDR3L-RS/ LPDDR3. | Ref |
| VCCST | Sustain voltage for the processor in standby modes | Ref |
| VIDSOUT<br>VIDSCLK<br>VIDALERT# | VIDALERT#, VIDSCLK, and VIDSCLK comprise a three signal serial synchronous interface used to transfer power management information between the processor and the voltage regulator controllers. | I/O CMOS<br>O CMOS<br>I CMOS |
| VR_EN | Sideband output from the processor which controls disabling of the VR when the processor is in the C10 state. This signal will be used to disable the VR only if the processor is configured to support VR disabling using VR_CURRENT_CONFIG MSR (601h). | O<br>VR Enable CMOS |
| VR_READY | Sideband signal which indicates to the processor that the external voltage regulator for the $V_{CC}$ power rail is valid. | I<br>CMOS |

## 6.11 Sense Signals

### Table 27. Sense Signals

| Signal Name | Description | Direction / Buffer Type |
|---|---|---|
| VCC_SENSE<br>VSS_SENSE | **VCC_SENSE and VSS_SENSE** provide an isolated, low-impedance connection to the processor input $V_{CC}$ voltage and ground. The signals can be used to sense or measure voltage near the silicon. | O<br>A |

## 6.12 Ground and Non-Critical to Function (NCTF) Signals

### Table 28. Ground and Non-Critical to Function (NCTF) Signals

| Signal Name | Description | Direction / Buffer Type |
|---|---|---|
| VSS | Processor ground node | GND |
| DAISY_CHAIN_NCTF _[Ball #]<br>(Y-Processor Line) | **Daisy Chain Non-Critical to Function:** These signals are for BGA solder joint reliability testing and are non-critical to function.<br>These signals are connected on the processor package as follows:<br>Package A1 Corner<br>• DAISY_CHAIN_NCTF_F1 to DAISY_CHAIN_NCTF_H2<br>• DAISY_CHAIN_NCTF_F3 to DAISY_CHAIN_NCTF_D2<br>Package A45 Corner<br>• DAISY_CHAIN_NCTF_A44 to DAISY_CHAIN_NCTF_C43<br>• DAISY_CHAIN_NCTF_D44 to DAISY_CHAIN_NCTF_F43<br>• DAISY_CHAIN_NCTF_F45 to DAISY_CHAIN_NCTF_C45<br>*Note:* Daisy_Chain_NCTF_H44 is not connected in package. | — |

## 6.13 Processor Internal Pull-Up / Pull-Down Terminations

### Table 29. Processor Internal Pull-Up / Pull-Down Terminations

| Signal Name | Pull Up / Pull Down | Rail | Value |
|---|---|---|---|
| BPM[7:0] | Pull Up | $Vcc_{IO}$ | 40–60 Ω |
| PREQ# | Pull Up | $Vcc_{IO}$ | 40–60 Ω |
| PROC_TDI | Pull Up | $Vcc_{ST}$ | 30–70 Ω |
| PROC_TMS | Pull Up | $Vcc_{ST}$ | 30–70 Ω |
| CFG[19:0] | Pull Up | $Vcc_{ST}$ | 5–8 kΩ |
| CATERR# | Pull Up | $Vcc_{ST}$ | 30–70 Ω |

# 7.0 Electrical Specifications

This chapter provides the processor electrical specifications including integrated voltage regulator (VR), $V_{CC}$ Voltage Identification (VID), reserved and unused signals, signal groups, Test Access Points (TAP), and DC specifications.

## 7.1 Integrated Voltage Regulator

A feature to the processor is the integration of platform voltage regulators into the processor. Due to this integration, the processor has one main voltage rail ($V_{CC}$) and a voltage rail for the memory interface ($V_{DDQ}$) , compared to six voltage rails on previous processors. The $V_{CC}$ voltage rail will supply the integrated voltage regulators which in turn will regulate to the appropriate voltages for the cores, cache, system agent, and graphics. This integration allows the processor to better control on-die voltages to optimize between performance and power savings. The processor $V_{CC}$ rail will remain a VID-based voltage with a loadline similar to the core voltage rail (also called $V_{CC}$) in previous processors.

## 7.2 Power and Ground Pins

The processor has VCC, VDDQ, and VSS (ground) pins for on-chip power distribution. All power pins must be connected to their respective processor power planes; all VSS pins must be connected to the system ground plane. Use of multiple power and ground planes is recommended to reduce I*R drop. The VCC pins must be supplied with the voltage determined by the processor **S**erial **V**oltage **ID**entification (SVID) interface. Table 30 on page 75 specifies the voltage level for the various VIDs.

## 7.3 $V_{CC}$ Voltage Identification (VID)

The processor uses three signals for the serial voltage identification interface to support automatic selection of voltages. The following table specifies the voltage level corresponding to the 8-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. See the *Voltage and Current Specifications* section for the DC specifications for these signals. The VID codes will change due to temperature and/or current load changes to minimize the power of the part. A voltage range is provided in the *Voltage and Current Specifications* section. 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 the *Voltage and Current Specifications* section. 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.

## Table 30. Voltage Regulator (VR) 12.5 Voltage Identification

| Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 | Hex | $V_{CC}$ |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 00h | 0.0000 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 01h | 0.5000 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 02h | 0.5100 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 03h | 0.5200 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 04h | 0.5300 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 05h | 0.5400 |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 06h | 0.5500 |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 07h | 0.5600 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 08h | 0.5700 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 09h | 0.5800 |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0Ah | 0.5900 |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0Bh | 0.6000 |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0Ch | 0.6100 |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0Dh | 0.6200 |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0Eh | 0.6300 |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0Fh | 0.6400 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 10h | 0.6500 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 11h | 0.6600 |
| 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 12h | 0.6700 |
| 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 13h | 0.6800 |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 14h | 0.6900 |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 15h | 0.7000 |
| 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 16h | 0.7100 |
| 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 17h | 0.7200 |
| 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 18h | 0.7300 |
| 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 19h | 0.7400 |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1Ah | 0.7500 |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1Bh | 0.7600 |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1Ch | 0.7700 |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1Dh | 0.7800 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1Eh | 0.7900 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1Fh | 0.8000 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 20h | 0.8100 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 21h | 0.8200 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 22h | 0.8300 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 23h | 0.8400 |
| 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 24h | 0.8500 |
| 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 25h | 0.8600 |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 26h | 0.8700 |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 27h | 0.8800 |
| 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 28h | 0.8900 |
| 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 29h | 0.9000 |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 2Ah | 0.9100 |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 2Bh | 0.9200 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 2Ch | 0.9300 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 2Dh | 0.9400 |
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 2Eh | 0.9500 |
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 2Fh | 0.9600 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 30h | 0.9700 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 31h | 0.9800 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 32h | 0.9900 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 33h | 1.0000 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 34h | 1.0100 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 35h | 1.0200 |
| 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 36h | 1.0300 |
| 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 37h | 1.0400 |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 38h | 1.0500 |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 39h | 1.0600 |
| 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 3Ah | 1.0700 |
| 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 3Bh | 1.0800 |
| 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 3Ch | 1.0900 |
| 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 3Dh | 1.1000 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 3Eh | 1.1100 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 3Fh | 1.1200 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 40h | 1.1300 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 41h | 1.1400 |

***continued...***

| Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 | Hex | $V_{CC}$ |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 42h | 1.1500 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 43h | 1.1600 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 44h | 1.1700 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 45h | 1.1800 |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 46h | 1.1900 |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 47h | 1.2000 |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 48h | 1.2100 |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 49h | 1.2200 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 4Ah | 1.2300 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 4Bh | 1.2400 |
| 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 4Ch | 1.2500 |
| 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 4Dh | 1.2600 |
| 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 4Eh | 1.2700 |
| 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 4Fh | 1.2800 |
| 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 50h | 1.2900 |
| 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 51h | 1.3000 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 52h | 1.3100 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 53h | 1.3200 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 54h | 1.3300 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 55h | 1.3400 |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 56h | 1.3500 |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 57h | 1.3600 |
| 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 58h | 1.3700 |
| 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 59h | 1.3800 |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 5Ah | 1.3900 |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 5Bh | 1.4000 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 5Ch | 1.4100 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 5Dh | 1.4200 |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 5Eh | 1.4300 |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 5Fh | 1.4400 |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 60h | 1.4500 |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 61h | 1.4600 |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 62h | 1.4700 |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 63h | 1.4800 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 64h | 1.4900 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 65h | 1.5000 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 66h | 1.5100 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 67h | 1.5200 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 68h | 1.5300 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 69h | 1.5400 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 6Ah | 1.5500 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 6Bh | 1.5600 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 6Ch | 1.5700 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 6Dh | 1.5800 |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 6Eh | 1.5900 |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 6Fh | 1.6000 |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 70h | 1.6100 |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 71h | 1.6200 |
| 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 72h | 1.6300 |
| 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 73h | 1.6400 |
| 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 74h | 1.6500 |
| 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 75h | 1.6600 |
| 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 76h | 1.6700 |
| 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 77h | 1.6800 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 78h | 1.6900 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 79h | 1.7000 |
| 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 7Ah | 1.7100 |
| 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 7Bh | 1.7200 |
| 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 7Ch | 1.7300 |
| 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 7Dh | 1.7400 |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 7Eh | 1.7500 |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 7Fh | 1.7600 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 80h | 1.7700 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 81h | 1.7800 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 82h | 1.7900 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 83h | 1.8000 |
| 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 84h | 1.8100 |
| 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 85h | 1.8200 |

***continued...***

| Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 | Hex | $V_{CC}$ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 86h | 1.8300 |
| 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 87h | 1.8400 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 88h | 1.8500 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 89h | 1.8600 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 8Ah | 1.8700 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 8Bh | 1.8800 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 8Ch | 1.8900 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 8Dh | 1.9000 |
| 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 8Eh | 1.9100 |
| 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 8Fh | 1.9200 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 90h | 1.9300 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 91h | 1.9400 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 92h | 1.9500 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 93h | 1.9600 |
| 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 94h | 1.9700 |
| 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 95h | 1.9800 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 96h | 1.9900 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 97h | 2.0000 |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 98h | 2.0100 |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 99h | 2.0200 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 9Ah | 2.0300 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 9Bh | 2.0400 |
| 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 9Ch | 2.0500 |
| 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 9Dh | 2.0600 |
| 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 9Eh | 2.0700 |
| 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 9Fh | 2.0800 |
| 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | A0h | 2.0900 |
| 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | A1h | 2.1000 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | A2h | 2.1100 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | A3h | 2.1200 |
| 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | A4h | 2.1300 |
| 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | A5h | 2.1400 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | A6h | 2.1500 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | A7h | 2.1600 |
| 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | A8h | 2.1700 |
| 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | A9h | 2.1800 |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | AAh | 2.1900 |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | ABh | 2.2000 |
| 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | ACh | 2.2100 |
| 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | ADh | 2.2200 |
| 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | AEh | 2.2300 |
| 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | AFh | 2.2400 |
| 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | B0h | 2.2500 |
| 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | B1h | 2.2600 |
| 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | B2h | 2.2700 |
| 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | B3h | 2.2800 |
| 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | B4h | 2.2900 |
| 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | B5h | 2.3000 |
| 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | B6h | 2.3100 |
| 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | B7h | 2.3200 |
| 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | B8h | 2.3300 |
| 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | B9h | 2.3400 |
| 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | BAh | 2.3500 |
| 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | BBh | 2.3600 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | BCh | 2.3700 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | BDh | 2.3800 |
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | BEh | 2.3900 |
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | BFh | 2.4000 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | C0h | 2.4100 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | C1h | 2.4200 |
| 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | C2h | 2.4300 |
| 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | C3h | 2.4400 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | C4h | 2.4500 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | C5h | 2.4600 |
| 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | C6h | 2.4700 |
| 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | C7h | 2.4800 |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | C8h | 2.4900 |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | C9h | 2.5000 |

***continued...***

| Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 | Hex | $V_{CC}$ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | CAh | 2.5100 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | CBh | 2.5200 |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | CCh | 2.5300 |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | CDh | 2.5400 |
| 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | CEh | 2.5500 |
| 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | CFh | 2.5600 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | D0h | 2.5700 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | D1h | 2.5800 |
| 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | D2h | 2.5900 |
| 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | D3h | 2.6000 |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | D4h | 2.6100 |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | D5h | 2.6200 |
| 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | D6h | 2.6300 |
| 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | D7h | 2.6400 |
| 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | D8h | 2.6500 |
| 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | D9h | 2.6600 |
| 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | DAh | 2.6700 |
| 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | DBh | 2.6800 |
| 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | DCh | 2.6900 |
| 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | DDh | 2.7000 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | DEh | 2.7100 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | DFh | 2.7200 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | E0h | 2.7300 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | E1h | 2.7400 |
| 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | E2h | 2.7500 |
| 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | E3h | 2.7600 |
| 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | E4h | 2.7700 |
| 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | E5h | 2.7800 |
| 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | E6h | 2.7900 |
| 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | E7h | 2.8000 |
| 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | E8h | 2.8100 |
| 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | E9h | 2.8200 |
| 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | EAh | 2.8300 |
| 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | EBh | 2.8400 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | ECh | 2.8500 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | EDh | 2.8600 |
| 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | EEh | 2.8700 |
| 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | EFh | 2.8800 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | F0h | 2.8900 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | F1h | 2.9000 |
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | F2h | 2.9100 |
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | F3h | 2.9200 |
| 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | F4h | 2.9300 |
| 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | F5h | 2.9400 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | F6h | 2.9500 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | F7h | 2.9600 |
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | F8h | 2.9700 |
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | F9h | 2.9800 |
| 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | FAh | 2.9900 |
| 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | FBh | 3.0000 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | FCh | 3.0100 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | FDh | 3.0200 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | FEh | 3.0300 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | FFh | 3.0400 |

*continued...*

## 7.4 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_TP – these signals should be routed to a test point

Arbitrary connection of these signals to VCC, VDDQ, VSS, or to any other signal (including each other) may result in component malfunction or incompatibility with future processors. See Signal Description on page 66 for a pin 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 (VSS). 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.

## 7.5 Signal Groups

Signals are grouped by buffer type and similar characteristics as listed in the following table. The buffer type indicates which signaling technology and specifications apply to the signals. All the differential signals and selected DDR3L / DDR3L-RS / LPDDR3 and Control Sideband signals have On-Die Termination (ODT) resistors. Some signals do not have ODT and need to be terminated on the board.

*Note:* All Control Sideband Asynchronous signals are required to be asserted/de-asserted for at least 10 BCLKs with maximum Trise/Tfall of 6 ns in order for the processor to recognize the proper signal state. See DC Specifications on page 81.

**Table 31. Signal Groups**

| Signal Group | Type | Signals |
|---|---|---|
| **Reference Clocks [2]** | | |
| Differential | DDR3L/DDR3L-RS Output | SA_CK[3:0], SA_CK#[3:0], SB_CK[3:0], SB_CK#[3:0] |
| | LPDDR3 Output | SA_CK[1:0], SA_CK#[1:0], SB_CK[1:0], SB_CK#[1:0] |
| **Command and Address Signals [2]** | | |
| Single ended | DDR3L/DDR3L-RS Output | SA_MA[15:0], SB_MA[15:0], SA_BS[2:0], SB_BS[2;0], SA_WE#, SB_WE#, SA_RAS#, SB_RAS#, SA_CAS#, SB_CAS# |
| | LPDDR3 Output | SA_CAA[9:0], SA_CAB[9:0], SB_CAA[9:0], SB_CAB[9:0] |
| **Control Signals [2]** | | |
| Single ended | DDR3L/DDR3L-RS Output | SA_CKE[3:0], SB_CKE[3:0], SA_CS#[3:0], SB_CS#[3:0], SA_ODT[3:0], SB_ODT[3:0] |
| | LPDDR3 Output | SA_CKE[3:0], SB_CKE[3:0], SA_CS#[1:0], SB_CS#[1:0], SA_ODT0, SB_ODT0 |
| **Data Signals [2]** | | |

*continued...*

| Signal Group | Type | Signals |
|---|---|---|
| Single ended | DDR3L/DDR3L-RS/ LPDDR3 Bi-directional | SA_DQ[63:0], SB_DQ[63:0] |
| Differential | DDR3L/DDR3L-RS/ LPDDR3 Bi-directional | SA_DQSP[7:0], SA_DQSN[7:0], SB_DQSP[7:0], SB_DQSN[7:0] |
| **Reference Voltage Signals** | | |
| Voltage | DDR3L/DDR3L-RS/ LPDDR3 Output | SM_VREF_CA, SM_VREF_DQ0, SM_VREF_DQ1 |
| **Testability (ITP/XDP)** | | |
| Single ended | GTL Input | PROC_TCK, PROC_TDI, PROC_TMS, PROC_TRST# |
| Single ended | GTL | PROC_TDO |
| Single ended | GTL | BPM#[7:0] |
| Single ended | GTL | PREQ# |
| Single ended | GTL | PRDY# |
| **Control Sideband** | | |
| Single ended | GTL Input/Open Drain Output | PROCHOT# |
| Single ended | Asynchronous CMOS Output | IVR_ERROR |
| Single ended | Open Drain Output | THERMTRIP# |
| Single ended | GTL | CATERR# |
| Single ended | Asynchronous CMOS Input | RESET#, PROCPWRGD, PWR_DEBUG# , VCCST_PWRGD |
| Single ended | Asynchronous Bi-directional | PECI |
| Single ended | GTL Bi-directional | CFG[19:0] |
| **Voltage Regulator** | | |
| Single ended | VR Enable CMOS Output | VR_EN |
| Single ended | CMOS Input | VR_READY |
| Single ended | CMOS Input | VIDALERT# |
| Single ended | Open Drain Output | VIDSCLK |
| Single ended | CMOS I/O | VIDSOUT |
| Differential | Analog Output | VCC_SENSE, VSS_SENSE |
| **Power / Ground / Other** | | |
| Single ended | Power | VCC, VDDQ, VCCST |
| | Ground | VSS |
| | No Connect | RSVD |
| | Test Point | RSVD_TP |
| | Other | DAISY_CHAIN_NCTF_[ball #] |

*continued...*

| Signal Group | Type | Signals |
|---|---|---|
| **Digital Display Interface** | | |
| Differential | DDI Output | DDIB_TXP[3:0], DDIB_TXN[3:0], DDIC_TXP[3:0], DDIC_TXN[3:0]] |
| *Notes:* 1. See Signal Description on page 66 for signal description details.<br>2. SA and SB refer to DDR3L / DDR3L-RS / LPDDR3 Channel A and DDR3L / DDR3L-RS / LPDDR3 Channel B. | | |

## 7.6 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. A few of the I/O pins may support only one of those standards.

## 7.7 DC Specifications

The processor DC specifications in this section are defined at the processor pins, unless noted otherwise. See Signal Description on page 66 for the processor pin listings and signal definitions.

- The DC specifications for the DDR3L / DDR3L-RS / LPDDR3 signals are listed in the *Voltage and Current Specifications* section.
- The *Voltage and Current Specifications* section lists the DC specifications for the processor and are valid only while meeting specifications for junction temperature, clock frequency, and input voltages. Read all notes associated with each parameter.
- AC tolerances for all DC rails include dynamic load currents at switching frequencies up to 1 MHz.
- All values are pre-silicon values and are subject to change.

## 7.8 Voltage and Current Specifications

### Table 32. Processor Core Active and Idle Mode DC Voltage and Current Specifications

| Symbol | Parameter | Segment | Min | Typ | Max | Unit | Note[1] |
|---|---|---|---|---|---|---|---|
| Operating Voltage | Voltage Range for Processor Active Operating Mode | All | 1.6 | — | 1.84 | V | 1, 2, 7 |
| Idle Voltage | Voltage Range for Processor Idle Mode (Package C6/C7) | All | 1.5 | — | 1.65 | V | 1, 2, 7 |
| $I_{CCMAX}$ | Maximum Processor Core $I_{CC}$ | Y-Processor Line | — | — | 18 | A | 4, 6, 7 |

*continued...*

| Symbol | Parameter | | Segment | Min | Typ | Max | Unit | Note[1] |
|---|---|---|---|---|---|---|---|---|
| $TOL_{VCC}$ | Voltage Tolerance | PS0, PS1 | All | — | — | ±20 | mV | 6, 8 |
| | | PS2, PS3 | | — | — | ±20 | | |
| Ripple | Ripple Tolerance | PS0 | All | — | — | ±15 | mV | 6, 8 |
| | | PS1 | | — | — | ±15 | | |
| | | PS2 | | — | — | +50/-15 | | |
| | | PS3 | | — | — | +60/-15 | | |
| R_DC_LL | Loadline slope within the VR regulation loop capability | | Y-Processor Line | — | -2.0 | — | mΩ | — |
| R_AC_LL | Loadline slope in response to dynamic load increase events | | Y-Processor Line | — | -7.0 | — | mΩ | — |
| T_OVS_Max | Maximum Overshoot time | | All | — | — | 500 | µs | — |
| V_OVS | Maximum Overshoot | | All | — | — | 200 | mV | — |

*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. Processor core VR to be designed to electrically support this current.
5. Processor core VR to be designed to thermally support this current indefinitely.
6. Long term reliability cannot be assured if tolerance, ripple, and core noise parameters are violated.
7. Long term reliability cannot be assured in conditions above or below Maximum/Minimum functional limits.
8. PSx refers to the voltage regulator power state as set by the SVID protocol.

## Table 33. Memory Controller ($V_{DDQ}$) Supply DC Voltage and Current Specifications

| Symbol | Parameter | Min | Typ | Max | Unit | Note |
|---|---|---|---|---|---|---|
| $V_{DDQ\ (DDR3L/DDR3L-RS)}$ | Processor I/O supply voltage for DDR3L/DDR3L-RS | — | 1.35 | — | V | 2, 3 |
| $V_{DDQ\ (LPDDR3)}$ | Processor I/O supply voltage for LPDDR3 | — | 1.20 | — | V | 2, 3 |
| $TOL_{DDQ}$ | VDDQ Tolerance (AC+DC) | -5 | — | 5 | % | 2, 3 |

*continued...*

| Symbol | Parameter | Min | Typ | Max | Unit | Note |
|---|---|---|---|---|---|---|
| $Icc_{MAX\_VDDQ\ (DDR3L/DDR3L\text{-}RS)}$ | Max Current for $V_{DDQ}$ Rail (DDR3L/DDR3L-RS) | — | — | 1.4 | A | 1 |
| $Icc_{MAX\_VDDQ\ (LPDDR3)}$ | Max Current for $V_{DDQ}$ Rail (LPDDR3) | — | — | 1.1 | A | 1 |

*Notes:* 1. The current supplied to the DIMM modules is not included in this specification.
2. Includes AC and DC error, where the AC noise is bandwidth limited to under 20 MHz.
3. No requirement on the breakdown of AC versus DC noise.

## Table 34. Vcc Sustain ($Vcc_{ST}$) Supply DC Voltage and Current Specifications

| Symbol | Parameter | Min | Typ | Max | Units | Notes |
|---|---|---|---|---|---|---|
| $Vcc_{ST}$ | Processor Vcc Sustain supply voltage | - 5% | 1.05 | + 5% | V | |
| $Icc_{MAX\_VccST}$ | Maximum Current for $Vcc_{ST}$ | — | — | 100 | mA | 1 |

*Note:* 1. The maximum $Icc_{MAX}$ specification is preliminary and based on initial silicon measurements and is subject to change.

## Table 35. DDR3L / DDR3L-RS Signal Group DC Specifications

| Symbol | Parameter | Min | Typ | Max | Units | Notes[1] |
|---|---|---|---|---|---|---|
| $V_{IL}$ | Input Low Voltage | — | $V_{DDQ}/2$ | $0.43*V_{DDQ}$ | V | 2, 4, 11, 14 |
| $V_{IH}$ | Input High Voltage | $0.57*V_{DDQ}$ | $V_{DDQ}/2$ | — | V | 3, 11, 14 |
| $V_{IL}$ | Input Low Voltage (SM_DRAMPWROK) | — | — | $0.15*V_{DDQ}$ | V | — |
| $V_{IH}$ | Input High Voltage (SM_DRAMPWROK) | $0.45*V_{DDQ}$ | — | 1.0 | V | 10, 12 |
| $R_{ON\_UP(DQ)}$ | DDR3L/DDR3L-RS Data Buffer pull-up Resistance | 20 | 26 | 32 | Ω | 5, 11 |
| $R_{ON\_DN(DQ)}$ | DDR3L/DDR3L-RS Data Buffer pull-down Resistance | 20 | 26 | 32 | Ω | 5, 11 |
| $R_{ODT(DQ)}$ | DDR3L/DDR3L-RS On-die termination equivalent resistance for data signals | 38 | 50 | 62 | Ω | 11 |
| $V_{ODT(DC)}$ | DDR3L/DDR3L-RS On-die termination DC working point (driver set to receive mode) | $0.45*V_{DDQ}$ | $0.5*V_{DDQ}$ | $0.55*V_{DDQ}$ | V | 11 |
| $R_{ON\_UP(CK)}$ | DDR3L/DDR3L-RS Clock Buffer pull-up Resistance | 20 | 26 | 32 | Ω | 5, 11, 13 |
| $R_{ON\_DN(CK)}$ | DDR3L/DDR3L-RS Clock Buffer pull-down Resistance | 20 | 26 | 32 | Ω | 5, 11, 13 |

***continued...***

| Symbol | Parameter | Min | Typ | Max | Units | Notes[1] |
|---|---|---|---|---|---|---|
| $R_{ON\_UP(CMD)}$ | DDR3L/DDR3L-RS Command Buffer pull-up Resistance | 15 | 20 | 25 | Ω | 5, 11, 13 |
| $R_{ON\_DN(CMD)}$ | DDR3L/DDR3L-RS Command Buffer pull-down Resistance | 15 | 20 | 25 | Ω | 5, 11, 13 |
| $R_{ON\_UP(CTL)}$ | DDR3L/DDR3L-RS Control Buffer pull-up Resistance | 19 | 25 | 31 | Ω | 5, 11, 13 |
| $R_{ON\_DN(CTL)}$ | DDR3L/DDR3L-RS Control Buffer pull-down Resistance | 19 | 25 | 31 | Ω | 5, 11, 13 |
| $R_{ON\_UP(SM\_PG\_CNTL1)}$ | System Memory Power Gate Control Buffer Pull-Up Resistance | 40 | 80 | 130 | Ω | 13 |
| $R_{ON\_DN(SM\_PG\_CNTL1)}$ | System Memory Power Gate Control Buffer Pull-Down Resistance | 40 | 80 | 130 | Ω | 13 |
| $I_{LI}$ | Input Leakage Current (DQ, CK)<br>0V<br>0.2*$V_{DDQ}$<br>0.8*$V_{DDQ}$ | — | — | 0.7 | mA | — |
| $I_{LI}$ | Input Leakage Current (CMD, CTL)<br>0V<br>0.2*$V_{DDQ}$<br>0.8*$V_{DDQ}$ | — | — | 1.0 | mA | — |
| SM_RCOMP0 | Command COMP Resistance | 198 | 200 | 202 | Ω | 8 |
| SM_RCOMP1 | Data COMP Resistance | 118.8 | 120 | 121.2 | Ω | 8 |
| SM_RCOMP2 | ODT COMP Resistance | 99 | 100 | 101 | Ω | 8 |

*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 in not controlled by the processor.
7. The minimum and maximum values for these signals are programmable by BIOS to one of the two sets.
8. SM_RCOMPx resistance must be provided on the system board with 1% resistors. SM_RCOMPx resistors are to $V_{SS}$.
9. SM_DRAMPWROK rise and fall time must be < 50 ns measured between $V_{DDQ}$ *0.15 and $V_{DDQ}$ *0.47.
10. SM_VREF is defined as $V_{DDQ}/2$.
11. Maximum-minimum range is correct; however, center point is subject to change during MRC boot training.
12. Processor may be damaged if $V_{IH}$ exceeds the maximum voltage for extended periods.
13. The MRC during boot training might optimize $R_{ON}$ outside the range specified.
14. $R_{ON}$ tolerance is preliminary and might be subject to change.

## Table 36. LPDDR3 Signal Group DC Specifications

| Symbol | Parameter | Min | Typ. | Max | Unit | Note |
|---|---|---|---|---|---|---|
| $V_{IL}$ | Input Low Voltage | — | $V_{DDQ}$ /2 | 0.43*$V_{DDQ}$ | V | 2, 4, 11, 12 |
| $V_{IH}$ | Input High Voltage | 0.57*$V_{DDQ}$ | $V_{DDQ}$ /2 | — | V | 3, 11, 12 |
| $V_{IL}$ | Input Low Voltage (SM_DRAMPWROK) | — | — | 0.15*$V_{DDQ}$ | V | — |
| $V_{IH}$ | Input High Voltage (SM_DRAMPWROK) | 0.45*$V_{DDQ}$ | — | 1.0*$V_{DDQ}$ | V | 10, 13 |
| $R_{ON\_UP(DQ)}$ | LPDDR3 Data Buffer pull-up Resistance | 30 | 40 | 50 | Ω | 5, 12 |
| $R_{ON\_DN(DQ)}$ | LPDDR3 Data Buffer pull-down Resistance | 30 | 40 | 50 | Ω | 5, 12 |
| $R_{ODT(DQ)}$ | LPDDR3 On-die termination equivalent resistance for data signals | 150 | 200 | 250 | Ω | 12 |
| $V_{ODT(DC)}$ | LPDDR3 On-die termination DC working point (driver set to receive mode) | 0.45*$V_{DDQ}$ | 0.5*$V_{DDQ}$ | 0.55*$V_{DDQ}$ | V | 12 |
| $R_{ON\_UP(CK)}$ | LPDDR3 Clock Buffer pull-up Resistance | 30 | 40 | 50 | Ω | 5, 12 |
| $R_{ON\_DN(CK)}$ | LPDDR3 Clock Buffer pull-down Resistance | 30 | 40 | 50 | Ω | 5, 12 |
| $R_{ON\_UP(CMD)}$ | LPDDR3 Command Buffer pull-up Resistance | 19 | 25 | 31 | Ω | 5, 12 |
| $R_{ON\_DN(CMD)}$ | LPDDR3 Command Buffer pull-down Resistance | 19 | 25 | 31 | Ω | 5, 12 |
| $R_{ON\_UP(CTL)}$ | LPDDR3 Control Buffer pull-up Resistance | 19 | 25 | 31 | Ω | 5, 12 |
| $R_{ON\_DN(CTL)}$ | LPDDR3 Control Buffer pull-down Resistance | 19 | 25 | 31 | Ω | 5, 12 |
| $R_{ON\_UP(RST)}$ | LPDDR3 Reset Buffer pull-up Resistance | 40 | 80 | 130 | Ω | — |
| $R_{ON\_DN(RST)}$ | LPDDR3 Reset Buffer pull-up Resistance | 40 | 80 | 130 | Ω | — |
| $I_{LI}$ | Input Leakage Current (DQ, CK)<br>0V<br>0.2* $V_{DDQ}$<br>0.8*$V_{DDQ}$ | — | — | 0.4 | mA | — |
| $I_{LI}$ | Input Leakage Current (CMD,CTL)<br>0V<br>0.2*$V_{DDQ}$<br>0.8*$V_{DDQ}$ | — | — | 0.6 | mA | — |
| SM_RCOMP0 | ODT COMP Resistance | 198 | 200 | 202 | Ω | 8 |

***continued...***

| Symbol | Parameter | Min | Typ. | Max | Unit | Note |
|---|---|---|---|---|---|---|
| SM_RCOMP1 | Data COMP Resistance | 118.8 | 120 | 121.2 | Ω | 8 |
| SM_RCOMP2 | Command COMP Resistance | 99 | 100 | 101 | Ω | 8 |

*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. RTERM 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 BIOS to one of the two sets.
8. SM_RCOMPx resistance must be provided on the system board with 1% resistors. SM_RCOMPx resistors are to VSS.
9. SM_DRAMPWROK must have a maximum of 15 ns rise or fall time over $V_{DDQ}$ * 0.30 ±100 mV and the edge must be monotonic.
10. SM_VREF is defined as $V_{DDQ}/2$
11. $R_{ON}$ tolerance is preliminary and might be subject to change.
12. Maximum-minimum range is correct; however, center point is subject to change during MRC boot training.
13. Processor may be damaged if $V_{IH}$ exceeds the maximum voltage for extended periods.

## Table 37. Digital Display Interface Group DC Specifications

| Symbol | Parameter | Min | Typ | Max | Units |
|---|---|---|---|---|---|
| $V_{IL}$ | HPD Input Low Voltage | — | — | 0.8 | V |
| $V_{IH}$ | HPD Input High Voltage | 2.25 | — | 3.6 | V |
| Vaux(Tx) | Aux peak-to-peak voltage at transmitting device | 0.39 | — | 1.38 | V |
| Vaux(Rx) | Aux peak-to-peak voltage at receiving device | 0.32 | — | 1.36 | V |

## Table 38. Embedded DisplayPort* (eDP) Group DC Specifications

| Symbol | Parameter | Min | Typ | Max | Units |
|---|---|---|---|---|---|
| $V_{OL}$ | eDP_DISP_UTIL Output Low Voltage | 0 | — | 0.1*VCC | V |
| $V_{OH}$ | eDP_DISP_UTIL Output High Voltage | 0.9*VCC | — | VCC | V |
| $R_{UP}$ | eDP_DISP_UTIL Internal pull-up | — | 100 | — | Ω |
| $R_{DOWN}$ | eDP_DISP_UTIL Internal pull-down | — | 100 | — | Ω |
| Vaux(Tx) | Aux peak-to-peak voltage at transmitting device | 0.39 | — | 1.38 | V |
| Vaux(Rx) | Aux peak-to-peak voltage at receiving device | 0.32 | — | 1.36 | V |
| eDP_RCOMP | COMP Resistance | 24.75 | 25 | 25.25 | Ω |

*Note:* 1. COMP resistance is to VCOMP_OUT.

## Table 39. CMOS Signal Group DC Specifications

| Symbol | Parameter | Min | Max | Units | Notes[1] |
|---|---|---|---|---|---|
| $V_{IL}$ | Input Low Voltage | — | $Vcc_{ST}$* 0.3 | V | 2 |
| $V_{IH}$ | Input High Voltage | $Vcc_{ST}$* 0.7 | — | V | 2, 4 |
| $R_{ON}$ | Buffer on Resistance | 30 | 70 | Ω | - |
| $I_{LI}$ | Input Leakage Current | — | ±150 | µA | 3 |

*Notes:*
1. Unless otherwise noted, all specifications in this table apply to all processor frequencies.
2. The $Vcc_{ST}$ referred to in these specifications refers to instantaneous VCCIO_OUT.
3. For VIN between “0” V and $Vcc_{ST}$. Measured when the driver is tri-stated.
4. $V_{IH}$ and $V_{OH}$ may experience excursions above $Vcc_{ST}$. However, input signal drivers must comply with the signal quality specifications.

## Table 40. GTL Signal Group and Open Drain Signal Group DC Specifications

| Symbol | Parameter | Min | Max | Units | Notes[1] |
|---|---|---|---|---|---|
| $V_{IL}$ | Input Low Voltage (TAP, except PROC_TCK, PROC_TRST#) | — | $Vcc_{ST}$* 0.6 | V | 2 |
| $V_{IH}$ | Input High Voltage (TAP, except PROC_TCK, PROC_TRST#) | $Vcc_{ST}$* 0.72 | — | V | 2, 4 |
| $V_{IL}$ | Input Low Voltage (PROC_TCK, PROC_TRST#) | — | $Vcc_{ST}$ * 0.3 | V | 2 |
| $V_{IH}$ | Input High Voltage (PROC_TCK, PROC_TRST#) | $Vcc_{ST}$ * 0.7 | — | V | 2, 4 |
| $V_{HYSTERESIS}$ | Hysteresis Voltage | $Vcc_{ST}$* 0.2 | — | V | — |
| $R_{ON}$ | Buffer on Resistance (TDO) | 7 | 17 | Ω | — |
| $V_{IL}$ | Input Low Voltage (other GTL) | — | $Vcc_{ST}$* 0.6 | V | 2 |
| $V_{IH}$ | Input High Voltage (other GTL) | $Vcc_{ST}$* 0.72 | — | V | 2, 4 |
| $R_{ON}$ | Buffer on Resistance (CFG/BPM) | 16 | 24 | Ω | — |
| $R_{ON}$ | Buffer on Resistance (other GTL) | 12 | 28 | Ω | — |
| $I_{LI}$ | Input Leakage Current | — | ±150 | µA | 3 |

*Notes:*
1. Unless otherwise noted, all specifications in this table apply to all processor frequencies.
2. The $Vcc_{ST}$ referred to in these specifications refers to instantaneous $Vcc_{ST}$.
3. For VIN between 0 V and $Vcc_{ST}$. Measured when the driver is tri-stated.
4. $V_{IH}$ and $V_{OH}$ may experience excursions above $Vcc_{ST}$. However, input signal drivers must comply with the signal quality specifications.

## Table 41. VR Enable CMOS Signal Group DC Specification

| Symbol | Parameter | Min | Max | Units | Notes |
|---|---|---|---|---|---|
| $R_{ON}$ | Buffer on Resistance | 30 | 70 | Ω | |
| $V_{HYSTERESIS}$ | Hysteresis Voltage | 0.15* $Vcc_{ST}$ | — | V | |

### Table 42. VCOMP_OUT and VCCIO_TERM

| Symbol | Parameter | Typ | Max | Units | Notes |
|---|---|---|---|---|---|
| VCOMP_OUT | Termination Voltage | 1.0 | — | V | 1, 3, 4 |
| VCCIO_TERM | Termination Voltage | 1.0 | — | V | 2 |

*Notes:* 1. VCOMP_OUT may only be used to connect eDP_RCOMP.
2. Internal processor power for signal termination.

## 7.8.1 Platform Environment Control Interface (PECI) DC Characteristics

The PECI interface operates at a nominal voltage set by $Vcc_{ST}$. The set of DC electrical specifications shown in the following table is used with devices normally operating from a $Vcc_{ST}$ interface supply.

$Vcc_{ST}$ nominal levels will vary between processor families. All PECI devices will operate at the $Vcc_{ST}$ level determined by the processor installed in the system.

### Table 43. Platform Environment Control Interface (PECI) DC Electrical Limits

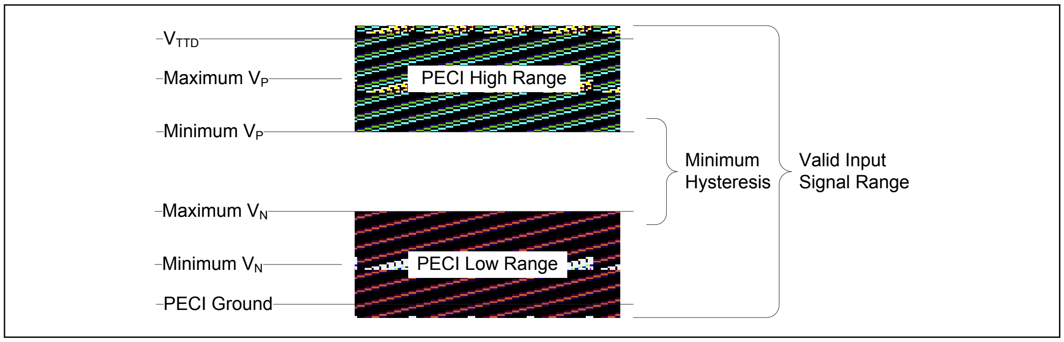
| Symbol | Definition and Conditions | Min | Max | Units | Notes[1] |
|---|---|---|---|---|---|
| $R_{up}$ | Internal pull up resistance | 15 | 45 | Ω | 3 |
| $V_{in}$ | Input Voltage Range | -0.15 | $Vcc_{ST}$ + 0.15 | V | — |
| $V_{hysteresis}$ | Hysteresis | 0.1 * $Vcc_{ST}$ | N/A | V | — |
| $V_n$ | Negative-Edge Threshold Voltage | 0.275 * $Vcc_{ST}$ | 0.525 * $Vcc_{ST}$ | V | — |
| $V_p$ | Positive-Edge Threshold Voltage | 0.550 * $Vcc_{ST}$ | 0.725 * $Vcc_{ST}$ | V | — |
| $C_{bus}$ | Bus Capacitance per Node | N/A | 10 | pF | — |
| $C_{pad}$ | Pad Capacitance | 0.7 | 1.8 | pF | — |
| Ileak000 | leakage current at 0 V | — | 0.6 | mA | — |
| Ileak025 | leakage current at 0.25* $Vcc_{ST}$ | — | 0.4 | mA | — |
| Ileak050 | leakage current at 0.50* $Vcc_{ST}$ | — | 0.2 | mA | — |
| Ileak075 | leakage current at 0.75* $Vcc_{ST}$ | — | 0.13 | mA | — |
| Ileak100 | leakage current at $Vcc_{ST}$ | — | 0.10 | mA | — |

*Notes:* 1. $Vcc_{ST}$ supplies the PECI interface. PECI behavior does not affect $Vcc_{ST}$ minimum / maximum specifications.
2. The leakage specification applies to powered devices on the PECI bus.
3. The PECI buffer internal pull-up resistance measured at 0.75* $Vcc_{ST}$.

## 7.8.2 Input Device Hysteresis

The input buffers in both client and host models must use a Schmitt-triggered input design for improved noise immunity. Use the following figure as a guide for input buffer design.

## Figure 13. Input Device Hysteresis



# 8.0 Package Specifications

## 8.1 Package Mechanical Attributes

The Y-Processor Line use a Flip Chip technology and Multi-Chip package (MCP) available in a Ball Grid Array (BGA) package. The following table provides an overview of the mechanical attributes of this package.

### Table 44. Package Mechanical Attributes

| | Parameter | Y-Processor Line |
|---|---|---|
| Package Technology | Package Type | Flip Chip Ball Grid Array |
| | Interconnect | Ball Grid Array (BGA) |
| | Lead Free | Yes |
| | Halogenated Flame Retardant Free | Yes |
| Package Configuration | Solder Ball Composition | SAC405 |
| | Ball/Pin Count | 1234 |
| | Grid Array Pattern | Balls Anywhere |
| | Land Side Capacitors | Yes |
| | Die Side Capacitors | No |
| | Die Configuration | Multi-Chip Package (MCP) / 2 dies |
| Package Dimension | Nominal Package Size | 30 mm x 16.5 mm x 1.05 mm |
| | Min Ball/Pin pitch | 0.5 mm |

*Note:* All values are pre-silicon values and are subject to change.

## 8.2 Package Loading Specifications

### Table 45. Package Loading Specifications

| Maximum Static Normal Load | Limit | Notes[4] |
|---|---|---|
| Y-Processor Line | 44 N (10 lbf) | 1, 2, 3 |

*Notes:*
1. The thermal solution attach mechanism must not induce continuous stress to the package. It may only apply a uniform load to the die to maintain a thermal interface.
2. This specification applies to the uniform compressive load in the direction perpendicular to the dies' top surface.
3. This specification is based on limited testing for design characterization.
4. All values are pre-silicon values and are subject to change.

## 8.3 Package Storage Specifications

### Table 46. Package Storage Specifications

| Parameter | Description | Min | Max | Notes[7] |
|---|---|---|---|---|
| $T_{\text{ABSOLUTE STORAGE}}$ | The non-operating device storage temperature. Damage (latent or otherwise) may occur when subjected to this temperature for any length of time. | -25 °C | 125 °C | 1, 2, 3 |
| $T_{\text{SUSTAINED STORAGE}}$ | The ambient storage temperature limit (in shipping media) for a sustained period of time. | -5 °C | 40 °C | 4, 5 |
| $RH_{\text{SUSTAINED STORAGE}}$ | The maximum device storage relative humidity for a sustained period of time. | 60% @ 24 °C | | 5, 6 |
| $TIME_{\text{SUSTAINED STORAGE}}$ | A prolonged or extended period of time: typically associated with customer shelf life. | 0 months | 6 months | 6 |

*Notes:*

1. Refers to a component device that is not assembled in a board or socket that is not to be electrically connected to a voltage reference or I/O signals.
2. Specified temperatures are based on data collected. Exceptions for surface mount reflow are specified by applicable JEDEC standards.
3. $T_{\text{ABSOLUTE STORAGE}}$ applies to the unassembled component only and does not apply to the shipping media, moisture barrier bags or desiccant.
4. Intel-branded board products are 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, 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.
5. The JEDEC, J-JSTD-020 moisture level rating and associated handling practices apply to all moisture sensitive devices removed from the moisture barrier bag.
6. Nominal temperature and humidity conditions and durations are given and tested within the constraints imposed by $T_{\text{SUSTAINED STORAGE}}$ and customer shelf life in applicable Intel boxes and bags.
7. All values are pre-silicon values and are subject to change.