Eagle Stream Platform

Electrical Data Sheet

Rev. 001

December 2024

Intel Confidential

Doc. No.: 814095, Rev.: 001

Notice: This document contains information on products in the design phase of development. The information here is subject to change without notice. Do not finalize a design with this information.

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

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

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

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

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

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

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

Intel, 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.

Contents

Figures

Tables

Revision History

Revision Number	Description	Date
1.0	• Initial release.	December 2024

1.0 Introduction

This document provides electrical specifications (including DC and AC electrical specifications, signal integrity, and land and signal definitions) of 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids.

NOTE

4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids is known herein after as the processor.

Features within this document may not be available on all platform segments, processor types, or processor SKUs. The data in the document is the most accurate information available by the publication date.

The processor supports up to 52 bits of physical address space and 48 bits of virtual address space. The processor is designed for a platform consisting of at least one server processor and the Platform Controller Hub (PCH). Included in this family of processors are Integrated Memory Controller (IMC) and an Integrated I/O (IIO) on a single silicon die.

Processor types support up to 80 lanes of PCI Express* 5.0 links capable of 32 GT/s and eight lanes of DMI. It features four Integrated Memory Controllers (IMC), each IMC supporting up to two channels of DDR5 DIMMs with up to two DIMMs per channel.

1.1 Related Publications

See the following documents for additional information.

Table 1. Related Publications

Document	Document Number/ Location
Intel® 64 and IA-32 Architectures Software Developer's Manuals Volume 1: Basic Architecture Volume 2A: Instruction Set Reference, A-M Volume 2B: Instruction Set Reference, N-Z Volume 3A: System Programming Guide Volume 3B: System Programming Guide Intel® 64 and IA-32Architectures Optimization Reference Manual	325462 http://www.intel.com/products/processor/manuals/index.htm
Intel® Virtualization Technology Specification for Directed I/O Architecture Specification	671081 http://www.intel.com/content/www/us/en/intelligent-systems/intel-technology/vt-directed-io-spec.html
Intel®Trusted Execution Technology Software Development Guide[1]	315168

continued...

Document	Document Number/ Location
	http://www.intel.com/technology/security/
Intel 4th Gen Intel Xeon Processor Scalable Family (Code name Sapphire Rapids) Data Sheet Vol 1-Architecture	814093
Intel 4th Gen Intel Xeon Processor Scalable Family (Code name Sapphire Rapids) Data Sheet Vol 2-Register	814094

NOTE

(1) - See the Resource & Documentation Center for an up-to-date collateral collection.

1.2 Statement of Volatility

4th Gen Intel® Xeon® Processor Scalable Family does not retain any end-user data aside from any SDSi based updates previously unlocked, when powered down and/or the processor is physically removed from the socket.

1.3 Terminology

Term	Description
BMC	Baseboard Management Controller.
CA	Coherency Agent. In some cases this is referred to as a Caching Agent though a CA is not actually required to have a cache. It is a term used for the internal logic providing mesh interface to LLC and Core.
CHA	The functional module that includes the Coherency Agent (CA) and Home Agent (HA).
DDR5	Fifth generation Double Data Rate SDRAM Memory technology.
DMI3	Direct Media Interface Gen3 operating at PCI Express* 3.0 speed.
DTS	Digital Thermal Sensor.
ECC	Error Correction Code.
Enhanced Intel SpeedStep® Technology	Allows the operating system to reduce power consumption when performance is not needed.
Execute Disable Bit	The Execute Disable bit allows memory to be marked as executable or non-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.
HA	A Home Agent (HA) orders read and write requests to a piece of coherent memory. The HA is implemented in the CHA logic.
IIO	Integrated I/O Controller. An I/O controller that is integrated in the processor die. The IIO consists of the DMI3 module, PCIe* modules, and MCP modules (Sapphire Rapids-F SKUs only).

continued...

Term	Description
IMC	Integrated Memory Controller. A memory controller that is integrated in the processor die.
Intel® 64Technology	64-bit memory extensions to the IA-32 architecture. Further details on Intel® 64 architecture and programming model can be found at http://developer.intel.com/technology/intel64/.
Intel® Turbo Boost Technology	A feature that opportunistically enables the processor cores to run at a faster frequency. This results in increased performance of both single and multi-threaded applications.
Intel® TXT	Intel® Trusted Execution Technology (Intel® TXT).
Integrated Heat Spreader (IHS)	A component of the processor package used to enhance the thermal performance of the package. Component thermal solutions interface with the processor at the IHS surface.
IVR	Integrated Voltage Regulation (IVR): The processor supports several integrated voltage regulators.
Intel® UPI	Intel® Ultra Path Interconnect (Intel® UPI) Agent. A cache-coherent, link-based Interconnect specification for Intel® processors and internal logic block providing interface between internal mesh and external Intel® UPI.
LLC	Last Level Cache.
M2M	Mesh to Memory. Logic in the IMC which interfaces the IMC to the mesh.
MESH	The on die interconnect which connects modules in the processor.
MLC	Mid Level Cache.
PCH	Platform Controller Hub. The next generation chipset with centralized platform capabilities including the main I/O interfaces along with display connectivity, audio features, power management, manageability, security and storage features.
PCU	Power Control Unit.
PCIe	PCI Express.
PECI	Platform Environment Control Interface.
Processor	Includes the 64-bit cores, uncore, I/Os and package.
Processor Core	The term “processor core” refers to the silicon (Si) die itself which can contain multiple execution cores. Each execution core has an instruction cache and data cache and MLC cache. All execution cores share the L3 cache.
Rank	A unit of DRAM corresponding four to eight devices in parallel, ignoring ECC. These devices are usually, but not always, mounted on a single side of a DDR5 DIMM.
RDIMM	Registered Dual In-line Memory Module.
RTID	Request Transaction IDs are credits issued by the CHA to track outstanding transaction, and the RTIDs allocated to a CHA are topology dependent.
SCI	System Control Interrupt. Used in ACPI protocol.
SKU	Stock Keeping Unit (SKU) is a subset of a processor type with specific features, electrical, power and thermal specifications. Not all features are supported on all SKUs. A SKU is based on specific use condition assumption.
SMBus	System Management Bus. A two-wire interface through which simple system and power management related devices can communicate with the rest of the system.
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.

continued...

Term	Description
	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.
TDP	Thermal Design Power - The maximum sustained processor power at its rated frequency. Used to determine the thermal solution envelope.
TSOD	Temperature Sensor On DIMM.
Uncore	The portion of the processor comprising the shared LLC cache, CHA, IMC, PCU, Ubox, IIO and Intel® UPI modules.
Unit Interval	Signaling convention that is binary and unidirectional. In this binary signaling, one bit is sent for every edge of the forwarded clock, whether it be a rising edge or a falling edge. If a number of edges are collected at instances t1, t 2, t n,...., then the UI at instance “n” is defined as: UI n = tn-t n-1.
x1, x4, x8, x16	Refers to a link or port with one, two, four or eight physical lane(s).

2.0 Electrical Specifications

This chapter describes processor signaling, AC and DC specifications, and signal quality. References to various interfaces (memory, PCIe*, Intel® Ultra Path Interconnect (Intel® UPI), PECI, and so forth) are also described.

2.1 Integrated Voltage Regulation

The processor has several voltage rails including: VCCIN, VCCINFAON, VCCFA_EHV, VCCFA_EHV_FIVRA, VCCD_HV, VCCVNN, P3V3_AUX for all SKUs and an additional VPP_HBM for SKUs with HBM.

2.2 Processor Signaling

The 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids includes 3647 lands, which utilize various signaling technologies. Signals are grouped by electrical characteristics and buffer type into various signal groups. These include DDR5 (Reference Clock, Command, Control, and Data), PCI Express*, DMI3, Intel® UPI, Platform Environmental Control Interface (PECI), System Reference Clock, SMBus, JTAG and Test Access Port (TAP), SVID Interface, Processor Asynchronous Sideband, Miscellaneous, and Power/ Other signals. See Table 8 on page 20 for details.

2.2.1 System Memory Interface Signal Groups

The system memory interface utilizes DDR5 technology, which consists of numerous signal groups. These include: Reference Clocks, Command Signals, Control Signals, Miscellaneous Signals and Data Signals. Each group consists of numerous signals, which may utilize various signaling technologies. See Table 8 on page 20 for further details.

Throughout this chapter the system memory interface may be referred to as DDR5.

2.2.2 PCI Express Signals

The PCI Express Signal Group consists of PCI Express ports 0, 1, 2, 3, and 4, and PCI Express miscellaneous signals. See Table 8 on page 20 for further details.

2.2.3 DMI3/PCI Express Signals

The Direct Media Interface Gen 3 (DMI3) sends and receives packets and/or commands to the PCH. The DMI3 is an extension of the standard PCI Express Specification. The DMI3/PCI Express Signals consist of DMI3 receive and transmit input/output signals and a control signal to select DMI3 or PCIe 4.0 operation for port 0. See Table 8 on page 20 for further details.

2.2.4 Intel Ultra Path Interconnect (Intel UPI)

Intel® Xeon® Processor Scalable Family two-socket provides two Intel® Ultra Path Interconnect (Intel® UPI) ports for high-speed serial transfer between other processors, whereas the 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids four-sockets and above provides three Intel® UPI links. Each port consists of two uni-directional links (for transmit and receive). A differential signaling scheme is utilized, which consists of opposite-polarity (DP, DN) signal pairs. See Table 8 on page 20 for further details.

2.2.5 Platform Environmental Control Interface (PECI)

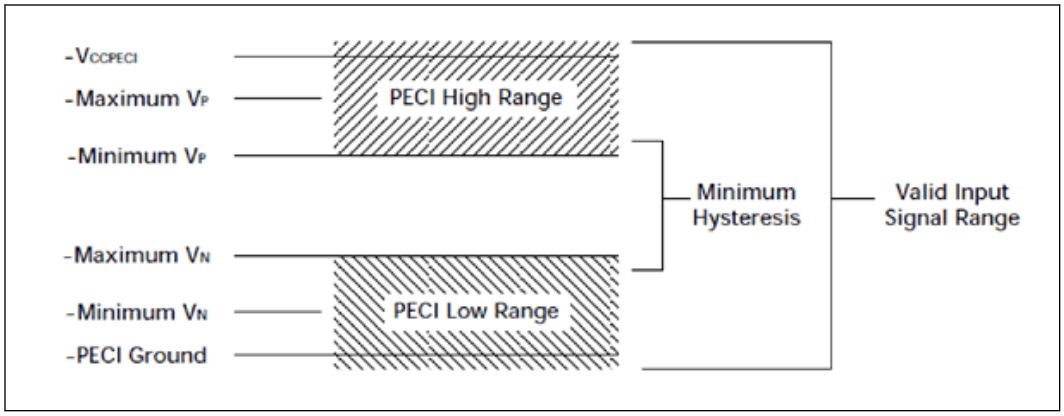
PECI is an Intel proprietary interface that provides a communication channel between Intel® processors and chipset components to external system management logic and thermal monitoring devices. The processor contains a Digital Thermal Sensor (DTS) that reports a relative die temperature as an offset from Thermal Control Circuit (TCC) activation temperature. Temperature sensors located throughout the die are implemented as analog-to-digital converters calibrated at the factory. PECI provides an interface for external devices to read processor temperature, perform processor manageability functions, and manage processor interface tuning and diagnostics.

The PECI interface operates at a nominal voltage. The set of DC electrical specifications shown in PECI DC Specifications on page 33 is used with devices normally operating from a PECI interface supply.

2.2.5.1 Input Device Hysteresis

The PECI client and host input buffers must use a Schmitt-triggered input design for improved noise immunity. Refer to the following image and PECI DC Specifications on page 33.

Figure 1. Input Device Hysteresis



2.2.6 System Reference Clocks (BCLK{0/1/2/3}_DP, BCLK{0/1/2/3}_DN)

The processor Core, processor Uncore, Intel® UPI, PCI Express and DDR5 memory interface frequencies are generated from BCLK{0/1/2/3}_DP and BCLK{0/1/2/3}_DN signals. There is no direct link between core frequency and Intel® UPI link frequency

(for example, no core frequency to Intel® UPI multiplier). The processor maximum core frequency, Intel® UPI link frequency and DDR memory frequency are set during manufacturing.

Clock multiplying within the processor is provided by the internal phase locked loop (PLL), which requires a constant frequency BCLK{0/1/2/3}_DP, BCLK{0/1/2/3}_DN input. DC specifications for the BCLK{0/1/2/3}_DP, BCLK{0/1/2/3}_DN inputs are provided in Processor Asynchronous Miscellaneous I/O DC Specifications on page 39.

These specifications must be met while also meeting the associated signal quality specifications outlined in Signal Quality on page 60.

Details regarding BCLK{0/1/2/3}_DP, BCLK{0/1/2/3}_DN driver specifications are provided in the CK404 Clock Synthesizer/Driver Specification.

2.2.7 JTAG and Test Access Port (TAP) Signals

Due to the voltage levels supported by other components in the JTAG and Test Access Port (TAP) logic, Intel recommends the processor be first in the TAP chain, followed by any other components within the system. Refer to the Sapphire Rapids Server Boundary Scan Description Language (BSDL) file more details. 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.

2.2.8 Processor Sideband Signals

Intel® Xeon® Processor Scalable Family includes asynchronous sideband signals that provide asynchronous input, output or I/O signals between the processor and the platform or Platform Controller Hub. Details can be found in Table 8 on page 20 and the applicable platform design guide.

All processor asynchronous sideband input signals are required to be asserted/deasserted for a defined number of BCLKs in order for the processor to recognize the proper signal state, these are outlined in Processor Asynchronous Miscellaneous I/O DC Specifications on page 39 and Processor Asynchronous Miscellaneous I/O AC Specifications on page 53. Refer to Signal Quality on page 60 for applicable signal integrity specifications.

2.2.9 Power, Ground and Sense Signals

Processors also include various other signals including power/ground and sense points. Details can be found in Table 8 on page 20 and the applicable platform design guide.

2.2.9.1 Power and Ground Lands

All lands must be connected to their respective processor power planes, while all VSS lands must be connected to the system ground plane.

For clean on-chip power distribution, processors include lands for all required voltage supplies. These are listed in the following table.

Table 2. Power and Ground Lands

Power and Ground Lands	Comments
VCCIN	Power input to FIVR powered by VR 14 on board. VCCIN voltage controlled by CPU's SVID Bus signals.
VCCINFAON	Power supply for the early on domains.
VCCFA_EHV	Power supply for the PCIe5, UPI IOs and all other FIVR.
VCCFA_EHV_FIVRA	Power supply for the analog IO FIVR.
VCCD_HV	Power supply for all processor DDR5 memory controllers.
VCCVNN	Power supply for the on-PKG device, CPU GPIOs for the future drop-in compatible CPU and platform GPIOs.
VCC_3P3_AUX	Power supply for the on package devices.
HBM_VPP	Power supply for HBM_VPP pins as a charge pump voltage for on-package HBM. For non-HBM SKUs, HBM_VPP pins are NC Inside the package.
VSS	Ground

2.2.9.2 Decoupling Guidelines

Due to its large number of transistors and high internal clock speeds, the processor is capable of generating large current swings between low and full power states. This may cause voltages on power planes to sag below their minimum values if bulk decoupling is not adequate. Large electrolytic bulk capacitors (CBULK), help maintain the output voltage during current transients, for example coming out of an idle condition. Care must be taken in the baseboard design to ensure that the voltages provided to the processor remain within the specifications. Failure to do so can result in timing violations or reduced lifetime of the processor.

2.2.9.3 Voltage Identification (VID)

The reference voltage or the VID setting is set via the SVID communication bus between the processor and the voltage regulator controller chip. The VID settings are the nominal voltages to be delivered to the processor's lands.

The processor uses voltage identification signals to support automatic selection of a power supply voltage. If the processor socket is empty (SKTOCC_N high), the voltage regulation circuit cannot supply the voltage that is requested and the voltage regulator must disable itself or not power on. VOUT_Max Register(30h) is recommended to be user programmable. CPU respects the Voltage value programmed in the VOUT_Max Register and does not issue any SetVID command above this defined value.

2.2.9.4 SVID Commands

The processor provides the ability to operate while transitioning to a new VID setting on its associated processor voltage rail. This is represented by a DC shift. It should be noted that a low-to-high or high-to-low voltage state change may result in as many VID transitions as necessary to reach the target voltage. Transitions above the maximum specified VID are not supported. The processor supports the following VR commands:

- SetVID_Fast (<=25 mV/µs for VCCIN, <=10 mV/uS for all other VRs on the SVID bus).
- SetVID_Slow is 1/4 or 1/2 of SetVID_Fast.

- SetVID_Decay not used.

The VRM or EVRD utilized must be capable of regulating its output to the value defined by the new VID.

Power source characteristics must be guaranteed to be stable whenever the supply to the voltage regulator is stable.

2.2.9.5 SetWP Working Point Command

The SetWP is a command that invokes a look up table for VID set points. During the initial power on phase the CPU will program the WPx registers (WP0=3Ah..WP7=41h) on a per rail address basis. When used with the AllCall address, SetWP acts as a group command that moves all voltage rails on the bus to new voltages. The SetWP command can also be used with an individual VR rail address and that rail moves to the voltage in the loop up table index. Each VR domain address has registers WP0-WPx (3Ah..41h) which stores the VID code for that domain's work points.

The Work Point command is encoded to support up to eight VID targets, slew rate for the command, and alert function. The PWM should use its auto power state or auto-phase shedding functions to select appropriate # phases, CCM/DCM operation, and so on, based on output load current after the SetWP command target has been reached.

Typical SetWP usage will be:

1. Processor writes VID codes to WP registers WP0 (3Ah) -WP4 (3Dh) in each VR domain. Normally done during SVID enumeration phase of system boot.
2. If a WP0-7 register is not programmed by the CPU, the VR stays at its present VID setting when it receives a SetWP (WPn) command.
3. Processor sends SetWP (WPn) command to one of the AllCall addresses 0Eh or 0Fh. See PWM guideline for more information on AllCall address mapping.
4. Voltage rails change VID to their corresponding VID code stored in their WPx register.
5. CPU polls each VR addresses reading stutus1 to clear the alerts from the VRs.
6. SVID error handling described in Serial VID Interface (SVID) Signals on page 66

WP0 = State 0, programed by master

WP1 = State 1, programmed by master

WP2 = State 2, programmed by master

WP3 = State 3, programmed by master

WP4 = State 4, programmed by master

...

WP7 = State 7

For the 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids, SetWP1 and SetWP2 commands are used.

2.2.9.6 SetVID Fast Command

The SetVID_Fast command contains the target VID in the payload byte. The range of voltage is defined in the VID table. The VR should ramp to the new VID setting with a fast slew rate as defined in the slew rate data register. It is maximum of 25 mV/µs for VCCIN and 10 mV/µs for other rails, depending on the amount of decoupling capacitance.

The SetVID_Fast command is preemptive. The VR interrupts its current processes and moves to the new VID. The SetVID_Fast command operates on 1 VR address at a time.

2.2.9.7 SetVID Slow

The SetVID_Slow command contains the target VID in the payload byte. The range of voltage is defined in the VID table. The VR should ramp to the new VID setting with a "slow" slew rate as defined in the slow slew rate data register. The SetVID_Slow is nominally 4x or 2x slower than the SetVID_Fast slew rate.

The SetVID_Slow command is preemptive, the VR interrupts its current processes and moves to the new VID. This is the instruction used for normal P-state voltage change. This command is used in the processor for the Enhanced Intel SpeedStep® Technology transitions.

2.2.9.8 SetVID Decay

The SetVID_Decay command is the slowest of the DVID transitions. It is only used for VID down transitions. The VR does not control the slew rate, the output voltage declines with the output load current only.

The SetVID_Decay command is preemptive, the VR interrupts its current processes and moves to the new VID. This command is used in the processor for package C6 entry, allowing capacitor discharge by the leakage, thus saving energy. This command is only used in VID down direction in the processor package C6 entry.

2.2.9.9 SVID Voltage Rail Addressing

The processor addresses five different voltage rail control segments within VR14/VR13 (VCCIN, VCCINFAON, VCCFA_EHV, VCCFA_EHV_FIVRA, VCCD_HV). The SVID data packet contains a 4-bit addressing code:

Table 3. SVID Address Usage Bus 0

PWM Address (HEX)	Protocol ID	4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids
00	0Ah (10 mV VR14 VID)	VCCIN
01	09h (5 mV VR14 VID)	VCCINFAON
02	04h (10 mV VR13 VID)	VCCFA_EHV
03	04h (10 mV VR13 VID)	VCCFA_EHV_FIVRA

Notes:
1. Check with VR vendors for determining the physical address assignment method for their controllers.
2. VR addressing is assigned on a per voltage rail basis.
3. Dual VR controllers will have two addresses with the lowest order address, always being the higher phase count.
4. For future platform flexibility, the VR controller should include an address offset, as shown with +1 not used.

Table 4. SVID Address Usage Bus 1

PWM Address (HEX)	Protocol ID	4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids
00	07h (5 mV VR13 VID)	VCCD_HV

Notes:
1. Check with VR vendors for determining the physical address assignment method for their controllers.
2. VR addressing is assigned on a per voltage rail basis.
3. Dual VR controllers will have two addresses with the lowest order address, always being the higher phase count.

Table 5. VCCIN Voltage Identification (VID)

SVID HEX	VCCIN SVID 10 mV Step Mode Voltage (V)	10 mV Step Recommended Accuracy
6F	1.60	±0.5% of VID
70	1.61	±0.5% of VID
71	1.62	±0.5% of VID
72	1.63	±0.5% of VID
73	1.64	±0.5% of VID
74	1.65	±0.5% of VID
75	1.66	±0.5% of VID
76	1.67	±0.5% of VID
77	1.68	±0.5% of VID
78	1.69	±0.5% of VID
79	1.70	±0.5% of VID
7A	1.71	±0.5% of VID
7B	1.72	±0.5% of VID
7C	1.73	±0.5% of VID
7D	1.74	±0.5% of VID
7E	1.75	±0.5% of VID
7F	1.76	±0.5% of VID
80	1.77	±0.5% of VID
81	1.78	±0.5% of VID
82	1.79	±0.5% of VID
83	1.80	±0.5% of VID
84	1.81	±0.5% of VID
85	1.82	±0.5% of VID
86	1.83	±0.5% of VID
87	1.84	±0.5% of VID
88	1.85	±0.5% of VID

continued...

SVID HEX	VCCIN SVID 10 mV Step Mode Voltage (V)	10 mV Step Recommended Accuracy
89	1.86	±0.5% of VID
8A	1.87	±0.5% of VID
8B	1.88	±0.5% of VID
8C	1.89	±0.5% of VID

NOTE

VID Range HEX 6F-86 are used by the 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids.

Table 6. VCCINFAON, VCCFA_EHV, VCCFA_EHV_FIVRA, VCCD_HV

SVID HEX	VCCINFAON SVID 5 mV Step Mode Voltage (V)	5 mV Step Recommended Accuracy	SVID HEX	VCCFA_EHV and VCCFA_EHV_FIVRA SVID 10 mV Step Mode Voltage (V)	10 mV Step Recommended Accuracy	SVID HEX	VCCD_HV SVID 5 mV Step Mode Voltage (V)	5 mV Step Recommended Accuracy
8D	0.950	± 5 mV	83	1.80	±0.5% of VID	AB	1.100	±0.5% of VID
8E	0.955	± 5 mV						
8F	0.960	± 5 mV						
90	0.965	± 5 mV						
91	0.970	± 5 mV						
92	0.975	± 5 mV						
93	0.980	±5 mV						
94	0.985	± 5 mV						
95	0.990	± 5 mV						
96	0.995	± 5 mV						
97	1.000	±0.5% of VID						

NOTE

DAC accuracy is a recommendation only. Total tolerance band must be met, that is, DAC set point + current sense AVP droop accuracy. See the applicable platform design guidelines for total tolerance band requirements.

2.2.10 Reserved or Unused Signals

All Reserved (RSVD) signals must not be connected. Connection of these signals to VCCIN, VCCD_HV, VSS, or to any other signal (including each other) can result in component malfunction or incompatibility with future processors.

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. Resistor values should be within ± 20% of the impedance of the baseboard trace, unless otherwise noted in the appropriate platform design guidelines.

2.3 Signal Group Summary

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.

Table 7. Signal Description Buffer Types

Signal	Description
Analog	Analog reference or output. May be used as a threshold voltage or for buffer compensation.
Asynchronous	Signal has no timing relationship with any system reference clock.
CMOS	CMOS Output buffers: 1.05V tolerant / CMOS Input buffers.
DDR5	CMOS Output buffers: 1.1V tolerant.
DMI3	Direct Media Interface Gen 3 signals. Non legacy DMI ports are compatible with PCI Express 4.0 Signaling Base and CEM Specifications.
Intel® UPI	Nominal voltage: 1.0V.
Open Drain	Open Drain buffers: 1.05V tolerant.
PCI Express	PCIe 5.0: These signals are compatible with PCI Express 5.0 Signaling Base and CEM Specifications and are AC coupled.
Reference	Voltage reference signal.
SSTL	Source Series Terminated Logic (JEDEC SSTL_15).

NOTE

Qualifier for a buffer type.

Table 8. Signal Groups

Differential/Single Ended	Buffer Type	Signal
DDR5 Reference Clocks		
Differential	SSTL Output	DDR{0/1/2/3/4/5/6/7}_CLK_D[N/P][1:0]

continued...

Differential/Single Ended	Buffer Type	Signal
DDR5 Command Signals		
Single-ended	SSTL Output	DDR{0/1/2/3/4/5/6/7}_SA_CA[6:0] DDR{0/1/2/3/4/5/6/7}_SB_CA[6:0] DDR{0/1/2/3/4/5/6/7}_SA_PAR DDR{0/1/2/3/4/5/6/7}_SB_PAR
DDR5 Control Signals		
Single-ended	SSTL Output	DDR{0/1/2/3/4/5/6/7}_SA_CS_N[3:0] DDR{0/1/2/3/4/5/6/7}_SB_CS_N[3:0]
DDR5 Data Signals		
Differential	SSTL Input/Output	DDR{0/1/2/3/4/5/6/7}_SA_DQS_D[N/P] [9:0] DDR{0/1/2/3/4/5/6/7}_SB_DQS_D[N/P] [9:0]
Single-ended	SSTL Input/Output	DDR{0/1/2/3/4/5/6/7}_SA_DQ[31:0] DDR{0/1/2/3/4/5/6/7}_SB_DQ[31:0] DDR{0/1/2/3/4/5/6/7}_SA_ECC[7:0] DDR{0/1/2/3/4/5/6/7}_SB_ECC[7:0]
DDR5 Miscellaneous Signals		
Single-ended	SSTL Input	DDR{0/1/2/3/4/5/6/7}_ALERT_N
	CMOS Input **Note:** Input voltage from platform cannot exceed 1.2V max.	DDR{01,23,45,67}_DRAM_PWR_OK DDR{0/1/2/3/4/5/6/7}_A_RSP[1:0] DDR{0/1/2/3/4/5/6/7}_B_RSP[1:0]
	CMOS 1.1V Output	DDR{01,23,45,67}_RESET_N
	Open Drain Output / CMOS Input	DDR[0123,4567]_SPDSCL DDR[0123,4567]_SPDSDA
PCI Express Port 0, 1, 2, 3, and 4 Signals		
Differential	PCI Express Input	PE{4:0}_RX_DN/DP[15:0]
Differential	PCI Express Output	PE{4:0}_TX_DN/DP[15:0]
PCI Express Miscellaneous Signals		
Single-ended	Open Drain Output	CXPSMBBUSSCL
Single-ended	Open Drain Output/CMOS Input	CXPSMBUSSDA
Single-ended	Open Drain Input	CXPSMBUS_ALERT_N
DMI3/PCI Express* Signals		
Differential	DMI3 Input	DMI_RX_D[N/P][7:0]
	DMI3 Output	DMI_TX_D[N/P][7:0]
Single-ended	DMI Miscellaneous	DMIMODE_OVERRIDE
Intel® UPI Signals		
Differential	Intel® UPI Input Output	UPI{3:0}_RX/TX_DN/DP[23:0]
Platform Environmental Control Interface (PECI)		
Single-ended	PECI Input/Output	PECI
System Reference Clock (BCLK{0/1/2/3}, XTAL_CLK)		

continued...

Differential/Single Ended	Buffer Type	Signal
Differential	Differential Input / CMOS Output	BCLK{0/1/2/3}_D[N/P]
Differential	Differential Input/ CMOS Output	XTAL_CLK
JTAG and TAP Signals		
Single ended	CMOS Input	TCK,TDI,TMS, PREQ_N
	Open Drain Output	TDO, PRDY_N
Serial VID Interface (SVID) Signals		
Single ended	CMOS Input	SVIDALERT{1/0}_N
	Open Drain Output / CMOS Input	SVIDDATA [1:0]
	Open Drain Output	SVIDCLK [1:0]
Processor Sideband Link		
Single ended		PMSYNC[6:0], PMDOWN[6:0], PMDOWN_PCH, PMSYNC_PCH
Processor Asynchronous Sideband Signals		
Single ended	CMOS Input	BIST_ENABLE, BMCINIT, LEGACY_SKT, NMI, TEST_PU_DA52, SOCKET_ID[2:0] FRMAGENT, PWRGOOD, RESET_N, SAFE_MODE_BOOT, TXT_AGENT TXT_PLTEN, PROCHOT_N
	Open Drain Output / CMOS Input	CATERR_N, MEMHOT_OUT_N, MEMHOT_IN_N, PMFAST_WAKE_N
	Open Drain Output	ERROR_N[2:0], THERMTRIP_N
	Not connected to Silicon	SKTOCC_N, PKG_ID[2:0], PROC_ID[1:0]
Power/Other Signals		
	Power / Ground	VCCIN, VCCINFAON, VCCFA_EHV, VCCFA_EHV_FIVRA, VCCD_HV, VCCVNN, VPP_HBM, VPP_HBM[4:1],VCC_3P3_AUX[1:0] and VSS
	Sense Points	VCCINFAON_SENSE VSS_VCCINFAON_SENSE, VCCFA_EHV_SENSE VSS_VCCFA_EHV_SENSE, VCCFA_EHV_FIVRA_SENSE VSS_VCCFA_EHV_FIVRA_SENSE, VCCD_HV_SENSE VSS_VCCD_HV_SENSE, VCCIN_SENSE, VSS_VCCIN_SENSE

Notes:

1. See Signal Descriptions on page 64 for signal description details.
2. DDR{0/1/2/3/4/5/6/7} refers to DDR5 Channel 0, DDR5 Channel 1, DDR5 Channel 2, DDR5 Channel 3, DDR5 Channel 4, DDR5 Channel 5, DDR5 Channel 6, and DDR5 Channel 7.

Table 9. Signals with On-Die Weak PU/PD

Signal Name	Pull Up/Pull Down	Rail	Value	Units	Notes
BIST_ENABLE	Pull Up	VCCVNN	3K-8K	ohm	-
BMCINIT	Pull Down	VSS	3K-8K	ohm	-
DMIMODE_OVERRIDE	Pull Up	VCCVNN	3K-8K	ohm	-
FBRK_N	Pull Up	VCCVNN	3K-8K	ohm	-
FRMAGENT	Pull Down	VSS	3K-8K	ohm	-
LEGACY_SKT	Pull Down	VSS	3K-8K	ohm	-
MEMHOT_IN_N	Pull Up	VCCVNN	3K-8K	ohm	-
NMI	Pull Down	VSS	3K-8K	ohm	-
PARTITION_ID[1:0]	Pull Down	VSS	3K-8K	ohm	-
PECI	Pull Down	VSS	3K-8K	ohm	-
PMDDOWN[6:0]	Pull Down	VSS	3K-8K	ohm	-
PMAX_TRIGGER_IO	Pull Down	VSS	3K-8K	ohm	-
PMFAST_WAKE_N	Pull Up	VCCVNN	3K-8K	ohm	-
PMSYNC[6:0]	Pull Down	VSS	3K-8K	ohm	-
TEST_PU_DA52	Pull Up	VCCVNN	3K-8K	ohm	-
PROCHOT_N	Pull Up	VCCVNN	3K-8K	ohm	-
SAFE_MODE_BOOT	Pull Down	VSS	3K-8K	ohm	-
SOCKET_ID[2:0]	Pull Down	VSS	3K-8K	ohm	-
TAP_ODT_EN	Pull Down	VSS	3K-8K	ohm	-
TCK	Pull Down	VSS	3K-8K	ohm	-
TDI	Pull Up	VCCVNN	3K-8K	ohm	-
TMS	Pull Up	VCCVNN	3K-8K	ohm	-
TXT_AGENT	Pull Down	VSS	3K-8K	ohm	-
TXT_PLTEN	Pull Up	VCCVNN	3K-8K	ohm	-

2.4 Mixing Processors

Intel supports and validates two, four, and eight-processor configurations only, where all processors share the same SKU and upgraded with the same On Demand features/ suite. Mixing components is not supported and will not be validated by Intel.

NOTE

No stepping mixing is supported.

The stepping ID is found in EAX[3:0] after executing the CPUID instruction with Function 01h. Details regarding the CPUID instruction are provided in the Intel® 64 and IA-32 Architectures Software Developer's Manuals, Volume 2A: Instruction Set Reference, A-M.

2.5 Flexible Motherboard Guidelines (FMB)

The Flexible Motherboard (FMB) guidelines are estimates of the maximum values the processor will have over certain time periods. The values are only estimates and actual specifications for future processors may differ. Processors may or may not have specifications equal to the FMB value in the foreseeable future. System designers should meet the FMB values to ensure their systems will be compatible with both the 4th Gen Intel® Xeon® Processor Scalable Family and 5th Gen Intel® Xeon® Processor Scalable Family.

2.6 Absolute Maximum and Minimum Ratings

The next table specifies the absolute maximum and minimum ratings. For conditions outside functional operation condition limits, but within absolute maximum and minimum ratings, neither functionality nor long-term reliability can be expected. If a device is returned to conditions within functional operation limits after having been subjected to conditions outside these limits, but within the absolute maximum and minimum ratings, the device may be functional, but with its lifetime degraded depending on exposure to conditions exceeding the functional operation condition limits. These values are often used for platform Voltage Regulator Overshoot and Undershoot protection settings to provide catastrophic VR failure protection.

Although the processor contains protective circuitry to resist damage from Electro-Static Discharge (ESD), precautions should always be taken to avoid high static voltages or electric fields.

Table 10. 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids Power Absolute Minimum and Maximum Voltage Ratings

Symbol	Parameter	Min.	Max.	Unit
VCCIN	SVID=1.8V/1.83V nom, input supply to FIVR, with respect to VSS.	-0.3	2.15	V
VCCINFAON	1V nom rail infrastructure Always-On (AON) for early on domains, with respect to VSS. This voltage is also used to power up the GPIO block, and will be used as reference for DC specifications.	-0.3	1.35	V
VCCFA_EHV	1.8V nom rail for PCIe 5.0, Intel UPI I/Os and all other FIVRs, with respect to VSS.	-0.3	2.15	V
VCCFA_EHV_FIVRA	Quiet fixed 1.8V nom voltage rail for the analog I/O FIVR and for the core power for On-Pkg HBM, with respect to VSS.	-0.3	2.15	V
VCCD_HV	1.1V nom rail for all processor DDR5 memory controllers only, not shared with DDR5 DIMMs, with respect to VSS.	-0.3	1.5	V
VNN_MAIN	1V nom rail used specifically to power the On-Pkg device and platform CPU GPIO terminations, with respect to VSS.	-0.3	1.35	V
3V3_AUX	3.3V nom rail used for the on Pkg devices. It is mandatory in both S5 (PIROM) and S0 states no matter if PIROM is supported or not, with respect to VSS.	-0.5	3.9	V
VPP_HBM	2.5V nom rail charge pump voltage for on-package HBM; this is mandatory only for any HBM enabled SKUs, with respect to VSS.	-0.3	3.0	V

Notes:

1. For functional operation, all processor electrical, signal quality, mechanical, and thermal specifications must be satisfied.
2. Overshoot and undershoot voltage guidelines for input, output, and I/O signals are outlined in Overshoot/Undershoot Tolerance on page 61. Excessive Overshoot or undershoot on any signal will likely result in permanent damage to the processor.

2.6.1 Storage Conditions Specifications

Environmental storage condition limits define the temperature and relative humidity limits to which the device is exposed to while being stored in a moisture barrier bag. The specified storage conditions are for component level prior to board attach (see notes in the following table for post board attach limits).

The following table specifies absolute maximum and minimum storage temperature limits which represent the maximum or minimum device condition beyond which damage, latent or otherwise, may occur. The table also specifies sustained storage temperature, relative humidity, and time-duration limits. These limits specify the maximum or minimum device storage conditions for a sustained period of time. At conditions outside sustained limits, but within absolute maximum and minimum ratings, quality and reliability may be affected.

Table 11. Storage Condition Ratings

Symbol	Parameter	Min.	Max.	Notes
Tabsolute storage	The non-operating device storage temperature. Damage (latent or otherwise) may occur when subjected to this temperature for any length of time in Intel® original sealed moisture barrier bad and / or box.	-25°C	125°C	1, 2, 3
Tsustained storage	The ambient storage temperature limit (in shipping media) for the sustained period of time as specified below in Intel® original sealed moisture barrier bad and /or box.	-5°C	40°C	1, 2, 3
RHsustained storage	The maximum device storage relative humidity for a sustained period of time as specified below in Intel® original sealed moisture barrier bag and / or box.	60% at 24°C		1, 2, 3
Time sustained storage	Maximum time: associated with customer shelf life in Intel® original sealed moisture barrier bag and / or box.	NA	Moisture Sensitive Devices: 60 months from bag seal date; Non-moisture sensitive devices: 60 months from lot date.	1, 2, 3

Notes:

1. TABSOLUTE STORAGE applies to the non-assembled only and does not apply to the shipping media, moisture barrier bag or desiccant. 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 re-flow are specified by applicable JEDEC J-STD-020 and MAS documents. The JEDEC, J-STD-020 moisture level rating and associated handling practices apply to all moisture sensitive devices removed from the moisture barrier bag.
3. Post board attach storage temperature limits are not specified for non Intel® branded boards. Consult your board manufacturer for storage specifications.

2.7 DC Specifications

DC Specifications are only valid while meeting specifications for case temperature (Tcase specified in the Intel Xeon Scalable Processors Thermal/Mechanical Specification and Design Guide), clock frequency and input voltages. Care should be taken to read all notes associated with each specification.

2.7.1 Voltage and Current Specifications

Table 12. The VCCIN Rail Current and Voltage Specifications for 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids

TDP / PL1 (W)	VCCIN _VID (V)	VCCIN _R_LL (mΩ)	IccIN_ Max (A)	IccIN_ Max. app (A)	IccIN_ PL1 (A)	PMax (W)	PMax.app (W)	VCCIN 2nd Droop Vmin (V)	VCCIN 3rd Droop Vmin (V)	VCCIN_VOvS_MAX for the First 25 µs (V)	Vtrip (V)
85	1.8	0.85	76	66	42	200	184	1.713	1.713	1.872	1.7199
95	1.8	0.85	91	79	48	222	204	1.701	1.701	1.872	1.7089
105	1.8	0.85	106	92	54	244	225	1.688	1.688	1.871	1.6978
125	1.8	0.85	141	119	66	298	267	1.658	1.658	1.870	1.6749
135	1.8	0.85	160	132	72	327	289	1.642	1.642	1.870	1.6638
145	1.8	0.85	180	146	78	358	311	1.625	1.625	1.869	1.6519
150	1.8	0.85	190	153	81	373	323	1.617	1.617	1.869	1.6460
155	1.8	0.85	201	160	84	389	334	1.607	1.607	1.868	1.6400
165	1.8	0.85	222	175	90	422	357	1.589	1.589	1.867	1.6273
185	1.8	0.85	266	204	102	490	405	1.572	1.556	1.866	1.6026
205	1.83	0.85	314	235	113	562	454	1.574	1.556	1.865	1.6063
225	1.83	0.5	364	266	122	638	504	1.626	1.626	1.863	1.6730
250	1.83	0.5	430	307	137	739	570	1.593	1.593	1.861	1.6525
270	1.83	0.5	485	341	149	824	624	1.594	1.576	1.861	1.6355
300	1.83	0.5	550	393	167	922	708	1.598	1.580	1.857	1.6095
330	1.83	0.5	550	430	185	922	764	1.598	1.580	1.855	1.5910
350	1.83	0.5	550	430	198	922	764	1.598	1.580	1.855	1.5910
385	1.83	0.5	550	430	220	922	764	1.598	1.580	1.855	1.5910
4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids + HMB SKUs											
330	1.83	0.5	550	430	185	1009	812	1.598	1.580	1.855	1.5910
350	1.83	0.5	550	430	198	1009	812	1.598	1.580	1.855	1.5910
Sapphire Rapids EE SKUs											
85	1.8	0.85	76	66	42	200	184	1.713	1.713	1.872	1.7199
95	1.8	0.85	91	79	48	222	204	1.701	1.701	1.872	1.7089
105	1.8	0.85	106	92	54	244	225	1.688	1.688	1.871	1.6978
110	1.8	0.85	119	102	59	265	241	1.677	1.677	1.871	1.6893
120	1.8	0.85	132	112	63	285	257	1.666	1.666	1.870	1.6808
125	1.8	0.85	141	119	66	298	267	1.658	1.658	1.870	1.6749
135	1.8	0.85	160	132	72	327	289	1.642	1.642	1.870	1.6638
140	1.8	0.85	170	139	75	343	300	1.634	1.634	1.869	1.6579
145	1.8	0.85	180	146	78	358	311	1.625	1.625	1.869	1.6519

continued...

TDP / PL1 (W)	VCCIN _VID (V)	VCCIN _R_LL (mΩ)	IccIN_ Max (A)	IccIN_ Max. app (A)	IccIN_ PL1 (A)	PMax (W)	PMax.app (W)	VCCIN 2nd Droop Vmin (V)	VCCIN 3rd Droop Vmin (V)	VCCIN_VOvS_MAX for the First 25 µs (V)	Vtrip (V)
150	1.8	0.85	190	153	81	373	323	1.617	1.617	1.869	1.6460
155	1.8	0.85	201	160	84	389	334	1.607	1.607	1.868	1.6400
160	1.8	0.85	212	168	87	406	346	1.598	1.598	1.867	1.6332
165	1.8	0.85	222	175	90	422	357	1.589	1.589	1.867	1.6273
185	1.8	0.85	266	204	102	490	405	1.572	1.556	1.866	1.6026
195	1.83	0.85	290	220	108	526	430	1.574	1.556	1.866	1.6190
205	1.83	0.85	314	235	113	562	454	1.574	1.556	1.865	1.6063
215	1.83	0.5	339	251	118	600	479	1.639	1.639	1.864	1.6805
225	1.83	0.5	364	266	122	638	504	1.626	1.626	1.863	1.6730
Sapphire Rapids EE E-Temp SKUs											
85	1.8	0.85	87	77	56	210	197	1.704	1.704	1.872	1.7106
95	1.8	0.85	106	93	63	239	219	1.687	1.687	1.871	1.6970
105	1.8	0.85	125	108	70	268	243	1.671	1.671	1.870	1.6842
110	1.8	0.85	140	120	75	291	260	1.659	1.659	1.870	1.6740
120	1.8	0.85	155	132	79	314	277	1.646	1.646	1.870	1.6638
125	1.8	0.85	165	139	83	329	289	1.638	1.638	1.869	1.6579
135	1.8	0.85	186	153	89	361	312	1.620	1.620	1.869	1.6460
140	1.8	0.85	195	160	91	376	324	1.612	1.612	1.868	1.6400
145	1.8	0.85	205	166	95	393	337	1.604	1.604	1.868	1.6349
150	1.8	0.85	215	173	98	409	349	1.595	1.595	1.867	1.6290
155	1.8	0.85	225	180	101	425	361	1.587	1.587	1.867	1.6230
160	1.8	0.85	236	187	104	442	373	1.577	1.577	1.866	1.6171
165	1.8	0.85	246	193	106	458	385	1.569	1.569	1.866	1.6120
185	1.8	0.85	286	216	116	526	435	1.568	1.552	1.865	1.5924
195	1.83	0.85	306	228	121	561	459	1.568	1.552	1.865	1.6122
205	1.83	0.5	343	253	132	596	485	1.636	1.636	1.865	1.6795
215	1.83	0.5	364	264	137	632	510	1.626	1.626	1.864	1.6740
225	1.83	0.5	404	292	148	668	536	1.606	1.606	1.864	1.6600

Power Parameter Definitions

Power Parameter Name	Definition	Notes
TDP	Thermal Design Power of the CPU.	The target power level CPU thermal solution should be designed to.
PL1	CPU Socket RAPL: Default Package Power Limit 1.	The default setting and the upper limit setting= TDP, set in MSR 610h.

continued...

TDP / PL1 (W)	VCCIN_VID (V)	VCCIN_R_LL (mΩ)	IccIN_Max (A)	IccIN_Max.app (A)	IccIN_PL1 (A)	PMax (W)	PMax.app (W)	VCCIN 2nd Droop Vmin (V)	VCCIN 3rd Droop Vmin (V)	VCCIN_VOvS_MAX for the First 25 µs (V)	Vtrip (V)
VccIN_VID				The Nominal VID During Normal Operation.							
VCCIN_R_LL				DC and AC Load Line, also known as AVP, Required.					The Platform R_LL setting should be based on the highest TDP SKUs supported by the platform.		
IccIN_Max				Max Current Corresponds to CPU PMax.							
IccIN_Max.app				Current Corresponds to CPU PMax.app.							
IccIN_PL1				Thermal Design Current Corresponds to CPU PL1 default Value.							
PMax				Instantaneous max CPU package power at virus condition.							
PMax.app				Instantaneous max CPU package power at the worst case real application condition.							
VCCIN 2nd Droop Vmin				The minimum Vmin during the rising edge of the transient current up to IccIN_Max, caused mainly by the Rpath and inductance of socket and board addressed by cavity caps.					Required for Fast Vmode validation with the current up to IccIN_Max.		
VCCIN 3rd Droop Vmin				The minimum Vmin at IccIN_Max level, addressed mainly by a mix of board caps in the cavity on top and bottom, the edge caps and VR tuning.					Required for Fast Vmode validation with the current up to IccIN_Max.		
VCCIN_VOvS_MAX				Maximum Overshoot voltage for the first 25 µs due to Load Transient release. After 25 µs, Vmax should meet AVP regulation (VccIN_VID-VCCIN_R_LL × Current + 22 mV).					Required for Transient 3D validation with the current up to IccIN_Max.app.		
Vtrip (V)				The fused PMax Detector Voltage Trip Level.					Calculated as: VccIN_VID-VCCIN_R_LL × IccIN_Max.app - 22 mV - 2 mV.		

NOTES

- All 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids + HBM and 5th Gen Intel® Xeon® Processor Scalable Family, Codename Emerald Rapids SKU numbers listed here were from pre-Si projection and subject to change.
- The voltage specification requirements are measured across the Gen5 VRTT test points. Voltage measurement should be taken with a DC to 20 MHz bandwidth (BW) oscilloscope limit (or DC to 100 MHz if 20 MHz BW oscilloscopes is not available), using a 1.5 pF maximum probe capacitance, and 1 MΩ minimum impedance. The maximum length of the ground wire on the probe should be less than 5 mm to ensure external noise from the system is not coupled in the scope probe.
- The processor should not be subjected to any static VCCIN level that exceeds the VCCIN_MAX (VccIN_VID-VCCIN_R_LL × Current + 22 mV) associated with any particular current. Failure to adhere to this specification can shorten processor lifetime.
- Minimum VCCIN and maximum ICCIN are specified at the maximum processor case temperature (TCASE). ICCIN_MAX is specified at the relative VCC_MIN point on the VCCIN load line.
- VCCIN has a Vboot setting of 1.8V.

Table 13. Other Processor Power Rail Current and Voltage Specifications for all 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids

Power Parameters	VCCINFAON	VCCFA_EHV	VCCFA_EHV _FIVRA	VCCD_HV	VCCVNN	VPP_HBM	3V3_AUX
Nominal Voltage =	1.0V	1.8V	1.8V	1.1V	1.0V	N/A	3.3V
TDC	42A	5A	SPR: 44A Future drop-in processor: 48A	SPR: 23A Future Drop-In processor: 26A	0.02A	N/A	0.4A
ICCMAX	46A	6.25A	SPR: 48Apk Future drop-in processor: 53Apk	SPR: 25Apk Future Drop-In processor: 30 Apk	0.02A	N/A	0.4A
Vmin measured at VRTT test points	0.930V at 1.0 Vnom	1.749V	See Table 14 on page 31	SPR: 1.086V; Future Drop-In processor: 1.081V	Rpath from VR output inductor to socket pin at the top layer is recommended = 120 mΩ 0.97 Vmin with calculation	N/A	3.205 Vmin with VRTT validation Rpath at the socket pin is recommended = 83 mΩ. 3.217 Vmin with calculation.
Vmax measured at VRTT test points	1.050V at 1.0 Vnom	1.841V	See Table 14 on page 31	SPR: 1.192 V Future Drop-In processor: 1.189V	Rpath from VR output inductor to socket pin at the top layer	N/A	3.395 Vmax with VRTT validation

continued...

Power Parameters	VCCINFAON	VCCFA_EHV	VCCFA_EHV _FIVRA	VCCD_HV	VCCVNN	VPP_HBM	3V3_AUX
					is recommended = 120 mΩ 1.03 Vmax with calculation		Rpath at the socket pin is recommended = 83 mΩ. 3.383 Vmax with calculation.
4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids + HBM SKUs							
Nominal Voltage =	1.0V	1.8V	1.8V	1.1V	1.0V	2.5V	3.3V
TDC	48A	5A	102A	23A	0.02A	4A	0.4A
ICCMAX	53A	6.25A	136A	25A	0.02A	5A	0.4A
Vmin measured at VRTT test points	0.909V at 1.0 Vnom	1.749V	See Table 14 on page 31	1.086V	Rpath from VR output inductor to socket pin at the top layer is recommended = 120 mΩ 0.97 Vmin with calculation	2.530V at 2.5 Vnom	3.205 Vmin with VRTT validation. Rpath at the socket pin is recommended = 83 mΩ. 3.217 Vmin with calculation.
Vmax measured at VRTT test points	1.050V at 1.0 Vnom	1.841V	See Table 14 on page 31	1.192V	Rpath from VR output inductor to socket pin at the top layer is recommended = 120 mΩ 1.03 Vmax with calculation	2.708V at 2.5 Vnom	3.395 Vmax with VRTT validation Rpath at the socket pin is recommended = 83 mΩ. 3.383 Vmax with calculation.

NOTES

- SPR = 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids.
- All 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids + HBM and 5th Gen Intel® Xeon® Processor Scalable Family, Codename Emerald Rapids SKU numbers listed here were from pre-Si projection and subject to change.
- The voltage specification requirements are measured across the Gen5 VRTT test points. Voltage measurement should be taken with a DC to 20 MHz bandwidth (BW) oscilloscope limit (or DC to 100 MHz if 20 MHz BW oscilloscopes is not available), using a 1.5 pF maximum probe capacitance, and 1 MΩ minimum impedance. The maximum length of the ground wire on the probe should be less than 5 mm to ensure external noise from the system is not coupled in the scope probe.
- PVNN_MAIN current on CPU side is 20 mA and too small to be tested with the black interposer. Measured the voltage at its VR output side, do Rpath simulation and calculate the Vmax/Vmin per: 1.0×(1+/-DC tolerance%) ±1/2 x Ripple pk-pk - Rpath x 0.02 and Vmax/Vmin spec is 1.03V/0.97V.
- Vmin and Vmax voltage includes: DC + AC + Ripple.

Table 14. VCCFA_EHV_FIVRA Voltage Specs Across 4 Quadrants and Remote Sense With Gen5 VRTT Test Points

Interposer Rails	Vmin	Vmax
For 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids Non-HBM SKUs		
VCCFA_EHV_FIVRA_NW	1.738V	1.864V
VCCFA_EHV_FIVRA_NE	1.704V	1.857V
VCCFA_EHV_FIVRA_SW	1.729V	1.865V
VCCFA_EHV_FIVRA_SE	1.713V	1.860V
VCCFA_EHV_FIVRA_RS	1.722V	1.862V
For Future Drop-In Non-HBM SKUs		
VCCFA_EHV_FIVRA_NW	1.739V	1.871V
VCCFA_EHV_FIVRA_NE	1.702V	1.859V
VCCFA_EHV_FIVRA_SW	1.730V	1.871V
VCCFA_EHV_FIVRA_SE	1.712V	1.864V
VCCFA_EHV_FIVRA_RS	1.720V	1.864V
For 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids + HBM SKUs		
VCCFA_EHV_FIVRA_NW	1.663V	1.866V
VCCFA_EHV_FIVRA_NE	1.660V	1.858V
VCCFA_EHV_FIVRA_SW	1.691V	1.844V
VCCFA_EHV_FIVRA_SE	1.685V	1.838V
VCCFA_EHV_FIVRA_RS	1.669V	1.831V

NOTE

All non-HBM Vmax/Vmin spec data is based on simulation with Fishhawk Falls 12L board and reduced caps, and all numbers listed here were from pre-Si projection and subject to change. All 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids + HBM and 5th Gen Intel® Xeon® Processor Scalable Family, Codename Emerald Rapids SKU numbers listed here were from pre-Si projection and subject to change.

2.7.2 Die Voltage Validation

Overshoot events in the VRTT testing must meet the specifications in Table 12 on page 26 for processor to meet its overshoot requirements when measured across the VCCIN_SENSE and VSS_VCCIN_SENSE lands.

2.7.3 Signal DC Specifications

For additional specifications, refer to Table 2.

2.7.3.1 DDR5 Signal DC Specifications

For the next table, use Signal Group Table 8 on page 20 to identify which signals belong to each group.

Symbol	Parameter	Min.	Nom.	Max.	Units	Notes[1]
IIL	Input Leakage Current	-1.4		+1.4	mA	9
Data Signals						
R ON	DDR5 Data Buffer On Resistance	30	37.5	45	Ω	6
Data ODT	On Die Termination	40	50	60	Ω	8
Reference Clock and Command Signals						
VOL	Output Low Voltage		Vol = (Ron / (Ron + RVDD_TERM)) ×VCCD		V	2, 7
VOH	Output High Voltage		VCCD		V	2, 5, 7, 11
Data Signals						
VOL	Output Low Voltage		Vol = (Ron / (Ron + RVDD_TERM)) ×VCCD			2,10
VOH	Output High Voltage		VCCD			2
Reference Clock Signal						
R ON	DDR5 Clock Buffer On Resistance	28	35	42	Ω	6
Command Signals						
R ON	DDR5 Command Buffer On Resistance	28	35	42	Ω	6

continued...

Symbol	Parameter	Min.	Nom.	Max.	Units	Notes[1]
VOL_CMOS1.1V	Output Low Voltage, Signals DDR_RESET_C{01/23}_N			$0.55\times V_{CCD}$	V	1, 2
V OH_CMOS1.1V	Output High Voltage, Signals DDR_RESET_C{01/23}_N	$0.95\times V_{CCD}$			V	1, 2
Control Signals						
R ON	DDR5 Control Buffer On Resistance	28	35	42	Ω	6
DDR5 Miscellaneous Signals						
DRAM{01/23/45/67}_PWR_OK						
R ON	DDR5 Reset Buffer On Resistance	35	45	55	Ω	6
VIL	Input Low Voltage		0.3 × VCCD		mV	2, 3
VIH	Input High Voltage		0.7 × VCCD		mV	2, 4, 5
ALERT_N						
VIL	Input Low Voltage	Vref -100		Vref -80	mV	3
VIH	Input High Voltage	Vref +80		Vref +100	mV	4
ODT	On Die Termination	56	70	84	Ω	

Notes:

1. Unless otherwise noted, all specifications in this table apply to all processor frequencies.
2. The voltage rail VCCD which will be set to 1.1V nominal depending on the voltage of all DIMMs connected to the processor.
3. VIL is the maximum voltage level at a receiving agent that will be interpreted as a logical low value.
4. VIH is the minimum voltage level at a receiving agent that will be interpreted as a logical high value.
5. VIH and VOH may experience excursions above VCCD. However, input signal drivers must comply with the signal quality specifications. Refer to Section 2.11 Signal Quality.
6. This is the pull down driver resistance. Refer to processor signal integrity models for I/V characteristics. Reset drive does not have a termination.
7. RVTT_TERM is the termination on the DIMM and not controlled by the processor. Refer to the applicable DIMM datasheet.
8. The minimum and maximum values for these signals are programmable by BIOS to one of the pairs.
9. Input leakage current is specified for all DDR5 signals.
10. Vol = Ron × [VCCD/(Ron + Rtt_Eff)], where Rtt_Eff is the effective pull-up resistance of all DIMMs in the system, including ODTs and series resistors on the DIMMs.
11. The VCCD value refers VCCD_HV power supply pins.

2.7.3.2 PECI DC Specifications

Symbol	Definition and Conditions	Min.	Max.	Units	Figure	Notes[1]
VIn	Input Voltage Range	-0.15	0.15 + VCCINFAON	V		1
VHysteresis	Hysteresis	0.1×VCCINFAON		V		
VIL Input Low Voltage	maximum voltage for low input	-	0.35×VCCINFAON	V		
VIH Input High Voltage	minimum voltage for high input	0.65×VCCINFAON	-	V		
VN	Negative-edge threshold voltage	0.275×VCCINFAON	0.500×VCCINFAON	V	Figure 1 on page 13	2
VP	Positive-edge threshold voltage	0.550×VCCINFAON	0.725×VCCINFAON	V	Figure 1 on page 13	2

continued...

Symbol	Definition and Conditions	Min.	Max.	Units	Figure	Notes[1]
I Source	Pullup Resistance (VOH = 0.75×VCCINFAON)	-6.00	-	mA		
ILeak+	High impedance state leakage to VCCINFAON (Vleak = VOL)	±10	±320	µA		3, 4
RPU	Pull up resistance	13.4	26.6	ohm		
CBus	Bus capacitance per node		10	pF		5
VNoise	Signal noise immunity above 300 MHz	0.100×VCCINFAON		Vp-p		
	Output Edge Rate (50Ω to VSS, between VIL and VIH)	5	15	V/ns		

Notes:

1. The input voltage range specifies an overshoot/undershoot that applies only to the PECI data signal and not to the VTT reference itself.
2. It is expected that the PECI driver will take into account, the variance in the receiver input thresholds and consequently, be able to drive its output within safe limits (-0.150 V to 275×VCCINFAON for the low level and 725×VCCINFAON to VCCINFAON+0.150V for the high level).
3. VCCINFAON nominal levels will vary between processor families. All PECI devices will operate at the VCCINFAON level determined by the processor installed in the system.
4. The leakage specification applies to powered devices on the PECI bus. Consider Min value to be at VIL/VIH while max value is at VCCINFAON.
5. Excessive capacitive loading on the PECI line may slow down the signal rise/fall times and consequently limit the maximum bit rate at which the interface can operate.

2.7.3.3 System Reference Clock (BCLK{0/1/2/3}) DC Specifications

Symbol	Parameter	Signal	Min.	Max.	Unit	Figure	Notes[1]
VIH	Differential Input High Voltage.	Differential.	0.150	-	V	Figure 2 on page 35	8
VIL	Differential Input Low Voltage.	Differential.	-	-0.150	V	Figure 2 on page 35	8
Vcross (abs)	Absolute Crossing Point.	Single Ended.	0.250	0.550	V	Figure 3 on page 35 and Figure 4 on page 36	2, 4, 8
Vcross (rel)	Relative Crossing Point.	Single Ended.	0.250 + 0.5×(VHavg - 0.700)	0.550 + 0.5×(VHavg - 0.700)	V	Figure 3 on page 35	3, 4, 5, 8
Vcross Delta	Range of Crossing Points.	Single Ended.	-	0.140	V	Figure 5 on page 36	2, 6, 8
VTH	Threshold Voltage.	Single Ended.	Vcross - 0.1	Vcross + 0.1	V		8
IIL	Input Leakage Current.	N/A		1.50	mA		7, 8

Notes:

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

continued...

Symbol	Parameter	Signal	Min.	Max.	Unit	Figure	Notes[1]

2. Crossing Voltage is defined as the instantaneous voltage value when the rising edge of BCLK{0/1/2/3}_DN is equal to the falling edge of BCLK{0/1/2/3}_DP.
3. VHavg is the single ended average voltage when BCLK is driven high.
4. The crossing point must meet the absolute and relative crossing point specifications simultaneously.
5. VHavg can be measured directly using "Vtop", "High" or other similar knob/feature in oscilloscopes.
6. VCROSS DELTA is defined as the total variation of all crossing voltages as defined in Note 2.
7. For Vin between 0 and Vih.
8. Specifications can be validated at the pin.

Figure 2. BCLK{0/1/2/3} Differential Clock Measurement Point for Ringback

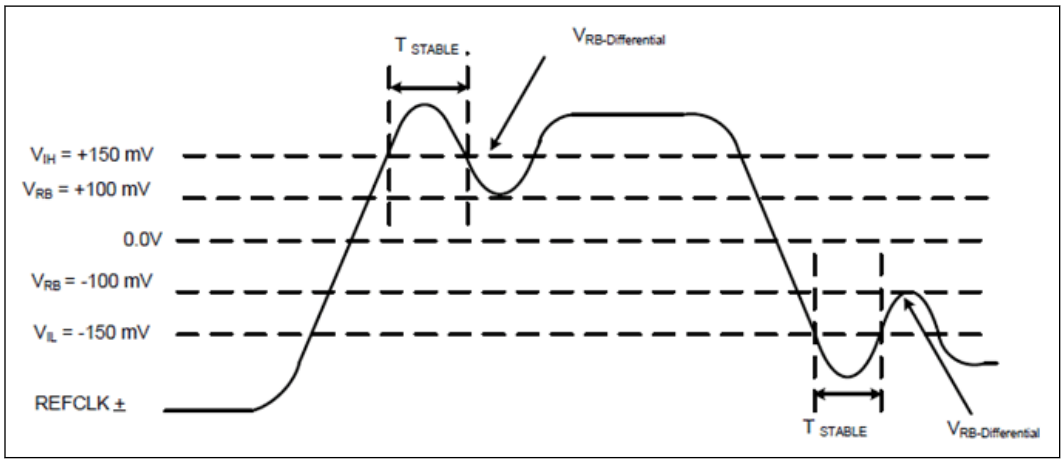


Figure 3. BCLK{0/1/2/3} Differential Clock Crosspoint Specification

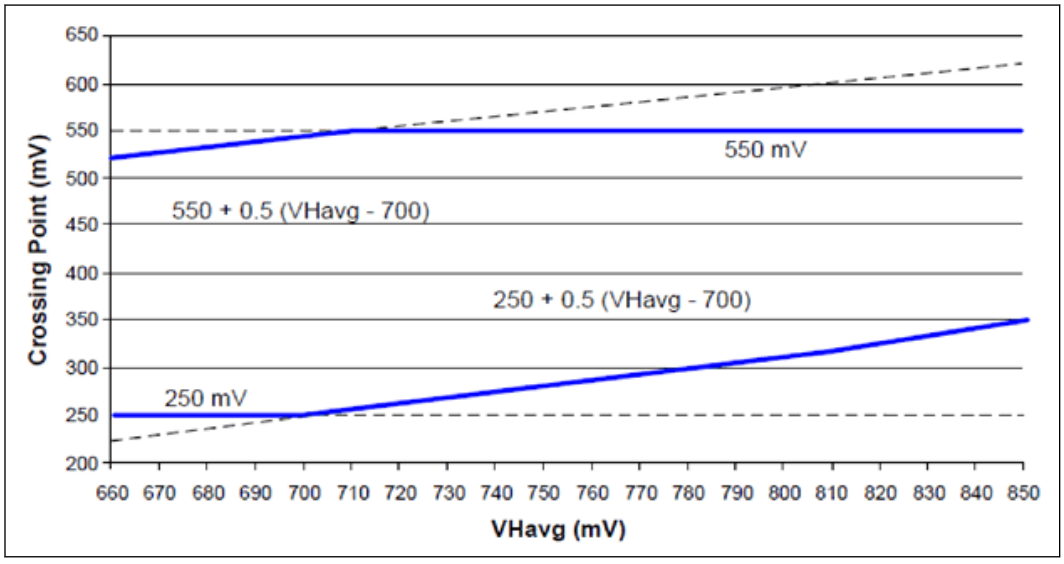


Figure 4. BCLK{0/1/2/3} Single Ended Clock Measurement Points for Absolute Cross Point and Swing

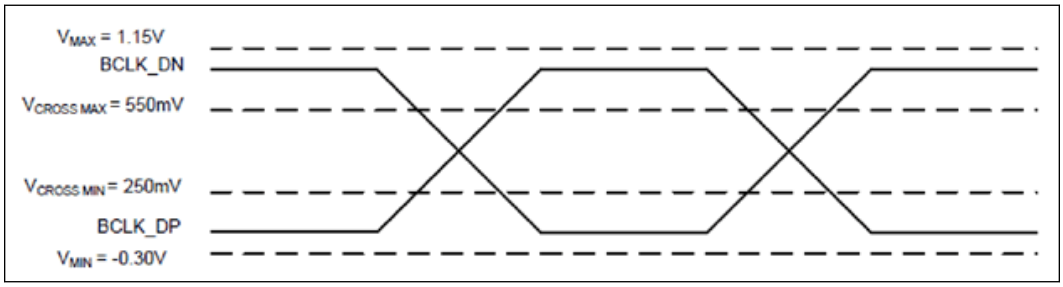
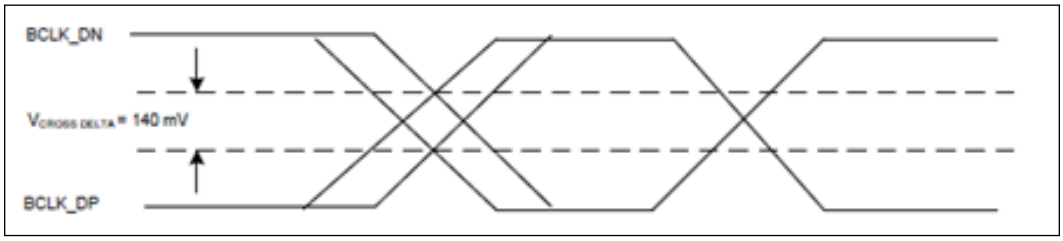


Figure 5. BCLK{0/1/2/3} Single Ended Clock Measure Points for Delta Cross Point



2.7.3.4 XTAL_CLK DC Specifications

Symbol	Parameter	Signal	Min.	Max.	Unit	Figure	Notes[1]
VIH	Differential Input High Voltage.	Differential.	0.150	-	V	Figure 2 on page 35	8, 9
VIL	Differential Input Low Voltage.	Differential.	-	-0.150	V	Figure 2 on page 35	8, 9
Vcross (abs)	Absolute Crossing Point.	Single Ended.	0.250	0.550	V	Figure 3 on page 35 and Figure 4 on page 36	2, 4, 8, 9
Vcross (rel)	Relative Crossing Point.	Single Ended.	0.250 + 0.5×(VH avg - 0.700)	0.550 + 0.5×(VH avg - 0.700)	V	Figure 3 on page 35	3, 4, 5, 8, 9
Vcross Delta	Range of Crossing Points.	Single Ended.	-	0.140	V	Figure 5 on page 36	6, 8, 9
VTH	Threshold Voltage.	Single Ended.	Vcross - 0.1	Vcross + 0.1	V		8
IIL	Input Leakage Current.	N/A		6	mA		7, 8

Notes:
1. Unless otherwise noted, all specifications in this table apply to all processor frequencies.
2. Crossing Voltage is defined as the instantaneous voltage value when the rising edge of XTAL_CLK_DN is equal to the falling edge of XTAL_CLK_DP.
3. VHavg is the single ended average voltage when XTAL_CLK is driven high.

continued...

Symbol	Parameter	Signal	Min.	Max.	Unit	Figure	Notes[1]
4. The crossing point must meet the absolute and relative crossing point specifications simultaneously. 5. VHavg can be measured directly using "Vtop", "High" or other similar knob/feature in oscilloscopes. 6. VCROSS DELTA is defined as the total variation of all crossing voltages as defined in Note 2. 7. For Vin between 0 and Vih. 8. Specifications can be validated at the pin. 9. BCLK figures are applicable to XTAL_CLK.							

2.7.3.5 SMBus DC Specifications

Symbol	Parameter	Min.	Max.	Units	Notes
VIL	Input Low Voltage.		0.35×VCCINFAON	V	
VIH	Input High Voltage.	0.65×VCCINFAON		V	
VHysteresis	Hysteresis.	0.1×VCCINFAON		V	
VOL Output Low Voltage	Maximum voltage for low input.		0.35×VCCINFAON		
VOH Output High Voltage	Minimum voltage for high input.	0.65×VCCINFAON			
RPD	Pull down resistance.	6.7	13.3	Ω	
IL	Leakage Current Signals.	±10	±320	µA	2
	Output Edge Rate (50Ω toVCCINFAON, between VIL and VIH).	1.13	5	V/ns	1

NOTES

1. Value obtained throught test bench with 50Ω pull-up to VCCINFAON.
2. Consider Min value to be at VIL/VIH with max value at VCCINFAON.

2.7.3.6 JTAG and TAP Signals DC Specifications

Symbol	Parameter	Min.	Max.	Units	Notes
VIL	Input Low Voltage: TCK.		0.35×VCCINFAON	V	
VIH	Input High Voltage: TCK.	0.65×VCCINFAON		V	
VIL	Input Low Voltage: TMS, TDI, PREQ_N, MBP_N[3:0].		0.45×VCCINFAON	V	
VIH	Input High Voltage: TMS, TDI, PREQ_N, MBP_N[3:0].	0.75×VCCINFAON		V	
VOL	Output Low Voltage: MBP[3:0], PRDY_N.		0.35×VCCINFAON	V	
VOL	Output Low Voltage: TDO.		0.25×VCCINFAON	V	

continued...

Symbol	Parameter	Min.	Max.	Units	Notes
VOH	Output High Voltage: TDO.		0.80×VCCINFAON	V	
VHysteresis	Hysteresis: TCK.	0.1×VCCINFAON			
VHysteresis	Hysteresis: TMS, TDI, PREQ_N, MBP[3:0].	0.08×VCCINFAON			
SRI	Input Slew Rate: TCK0, TCK1, MBP[3:0]_N, TDI.	0.05		V/ns	1,2
RPD	Buffer On Resistance Signals MBP[3:0]_N, PRDY_N, TDO.	4	8	Ω	3
IL	Input Leakage Current Signals.	±10	±320	µA	4
SRO	Output Edge Rate Signal: MBP[3:0]_N, PRDY_N, TDO.		1	V/ns	5

Notes:
1. These are measured between VIL and VIH.
2. The signal edge rate must be met or the signal must transition monotonically to the asserted state.
3. ±30% overall range.
4. Consider Min value to be at VIL/VIH while max value is at VCCINFAON.
5. These are measured between VOL and VOH.

2.7.3.7 Serial VID Interface (SVID) DC Specifications

Symbol	Parameter	Min	Nom	Max	Units	Notes
V IL	Input Low Voltage Signals: SVIDCLK, SVIDDATA, SVIDALERT_N.			0.35×VCCINFAON	V	1
VIH	Input High Voltage Signals: SVIDCLK, SVIDDATA, SVIDALERT_N.	0.65×VCCINFAON			V	1
VOL	Output Low Voltage Signals: SVIDCLK, SVIDDATA.			0.35×VCCINFAON	V	1, 6
VOH	Output Low Voltage Signals: SVIDCLK, SVIDDATA.	0.65×VCCINFAON				
VHysteresis	Hysteresis.	0.1×VCCINFAON			V	1
RPD	Pull down Resistance for signals SVIDCLK, SVIDDATA.	8.4		16.6	Ω	2
IL	Input Leakage Current.	±10		±320	µA	3,4
	Input Edge Rate Signal: SVIDALERT_N.	0.05			V/ns	5
	Output Edge Rate.	1.13		5	V/ns	5, 6

Notes:
1. Refers to instantaneous VCCINFAON.
2. Measured at VIL
3. Vin between 0V and VCCINFAON (applies to SVIDDATA and SVIDALERT_N only). Consider the Min value to be at VIL/VIH while the max value is at VCCINFAON.
4. See the *Eagle Stream Platform Design Guide*, document number 610826, for routing design guidelines.
5. These are measured between VIL and VIH.
6. Value obtained through test bench with a 50Ω pull up toVCCINFAON.

2.7.3.8 Processor Asynchronous Miscellaneous I/O DC Specifications

Symbol	Parameter	Min.	Max.	Units	Notes
CMOS output buffers					
IL	Input Leakage Current	±10	±320	µA	1,2,4
VOL	Low Output Voltage		0.35×VCCINFAON	V	1,2,4
VOH	High Output Voltage	0.65×VCCINFAON		V	1,2,4
RPD	Pull down Resistance	33.5	66.5	Ω	1,2,4,6
RPU	Pull up Resistance:	33.5	66.5	Ω	1,2,4,6
SR	Output Edge Rate: Signal: MEM_HOT_C{01/23}_ N, ERROR_N[2:0], THERMTRIP, PROCHOT_N	0.8	3	V/ns	
CMOS input buffers					
VIL	Input Low Voltage		0.35×VCCINFAON	V	1, 2,4
VIH	Input High Voltage	0.65×VCCINFAON		V	1, 2,4
VHysteresis	Hysteresis Signals	0.1		V	1,2,4
SRI	Input Slew Rate	0.005		V/ns	
Open Drain Output buffers					
IL	Input Leakage Current	±10	±320	µA	1,2,4
RPD	Pull down resistance	8.4	16.6	Ω	1,2,4
SR	Output Edge Rate	1.13	5	V/ns	3,5

Notes:

1. This table applies to the processor miscellaneous signals specified in Table 8 on page 20. For IL consider the Min value to be at VIL/VIH while the max value is at VCCINFAON.
2. Unless otherwise noted, all specifications in this table apply to all processor frequencies.
3. These are measured between VIL and VIH.
4. In the case of bidirectional signals they use either a CMOS output/CMOS input buffer or they use Open Drain/CMOS input buffer.
5. VOL level for open drain buffers may be obtained with the Buffer ON Resistance and the external 50Ω pull up to VCCINFAON.
6. This instance applies to one buffer and must be divided by the corresponding buffer number for dual or quad buffer.

2.7.3.9 Miscellaneous Signals DC Specifications

Symbol	Parameter	Min.	Nominal	Max.	Units	Notes
SKTOCC_N Signal						
VO_ABS_MAX	Output Absolute Max Voltage.		3.30	3.50	V	1
IOMAX	Output Max Current.			2	mA	2

2.7.3.10 SBLINK DC Specifications

This section describes the DC Specifications for the SBLINK.

Symbol	Parameter	Min.	Max.	Units	Notes2
IL	Input Leakage Current	±10	±320	µA	1
VOL	Low Output Voltage		0.35×VCCINFAON	V	
VOH	High Output Voltage	0.65×VCCINFAON		V	
RPD (PMDOWN_PCH)	Pull down Resistance	16.75	33.25	Ω	
RPU (PMDOWN_PCH)	Pull up Resistance	16.75	33.25	Ω	
RPD (PMDOWN[6:0])	Pull down Resistance	33.5	66.5	Ω	
RPU (PMDOWN[6:0])	Pull up Resistance	33.5	66.5	Ω	
RPD (PMSYNC[6:0])	Pull down Resistance	8.4	16.6	Ω	
RPU (PMSYNC[6:0])	Pull up Resistance	8.4	16.6	Ω	
VIL	Input Low Voltage		0.35×VCCINFAON	V	
VIH	Input High Voltage	0.65×VCCINFAON		V	
VHysteresis	Hysteresis Signals	0.1		V	

Notes:
1. For IL consider the Min value to be at VIL/VIH while max value is at VCCINFAON.
2. Unless otherwise noted, all specifications in this table apply to all processor frequencies.

2.8 AC Specifications

AC specifications are defined at the processor pads, unless otherwise noted. Therefore, proper simulation is the only means to verify proper timing and signal quality. Timings specified in this section should be used in conjunction with processor signal integrity models provided by Intel. Care should be taken to read all notes associated with each parameter.

For additional specifications, refer to Related Publications on page 8.

For the next table, use Signal Group Table 8 on page 20 to identify which signals belong to each group.

2.8.1 DDR5 Signals AC Specifications

Symbol	Parameters	Channel 0, 1, 2, 3, 4, 5, 6, and 7			Unit	Figure	Note[1]
		Min.	Nom.	Max.			
Latency Timings							
tCL - tRCD - tRP	CAS Latency - RAS to CAS Delay - Pre-charge Command Period.	4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids 4000 MT/s: 28-28-28; 32-32-32; 32-32-32; 36-35-35; 4400 MT/s: 32-32-32; 36-36-36; 36-36-36; 40-39-39; 4800 MT/s: 34-34-34; 40-39-39; 40-40-40; 42-42-42; 5th Gen Intel® Xeon® Processor Scalable Family, Codename Emerald Rapids 4800 MT/s: 34-34-34; 40-39-39; 40-40-40; 42-42-42; 5200 MT/s: 38-38-38; 42-42-42; 42-42-42; 46-46-46; 5600 MT/s: 40-40-40; 46-45-45; 46-46-46; 50-49-49;			tCK		
Electrical Characteristics							
Clock Timings							
tCK	tCK (AVG).		4000: 500.00 4400: 454.55 4800: 416.67 5200: 384.62 5600: 357.14		ps		7
TCH	CLK High Time.	0.45×TCK		0.55×TCK	ns		
TCL	CLK Low Time.	0.45×TCK		0.55×TCK	ns		
TSKEW	Skew Between Any System Memory Differential Clock Pair (CLK_P/CLK_N).			155	ps		
Data and Strobe Signal Timings							
UI	Unit Interval.		0.5×TCK		UI		
(TDVA+ TDVB)	DQ[63:0] Valid before and after DQS_DN[17:0] Rising or Falling Edge.			0.85	UI		5
(TDQS_CO)	DQS_DN Edge Placement Accuracy to CK Rising Edge Adjustable Range.	-1.0		1.0	UI		6

continued...

Symbol	Parameters	Channel 0, 1, 2, 3, 4, 5, 6, and 7			Unit	Figure	Note[1]
		Min.	Nom.	Max.			
(TWPRE)	DQS_DN/DQS_DP Write Preamble Duration.		2, 3, 4		TCK		
(TWPST)	DQS_DN/DQS_DP Write Postamble Duration.		0.5 / 1.5		TCK		

Notes:

1. Unless otherwise noted, all specifications in this table apply to all processor frequencies. Timing specifications only depend on the operating frequency of the memory channel and not the maximum rated frequency.
2. Edge Placement Accuracy (EPA): The silicon contains digital logic that automatically adjusts the timing relationship between the DDR reference clocks and DDR signals. The BIOS initiates a training procedure that will place a given signal appropriately within the clock period. The difference in delay between the signal and clock is accurate to within ±EPA. This EPA includes jitter, skew, within die variation and several other effects.
3. Data to Strobe read setup and Data from Strobe read hold minimum requirements specified at the processor pad are determined with the minimum Read DQS_DN/DQS_DP delay.
4. The system memory clock outputs are differential (CLK_DN and CLK_DP), the CLK_DN rising edge is referenced at the crossing point where CLK_DN is rising and CLK_DP is falling.
5. The system memory strobe outputs are differential (DQS_DN and DQS_DP), the DQS_DN rising edge is referenced at the crossing point where DQS_DN is rising and DQS_DP is falling, and the DQS_DN falling edge is referenced at the crossing point where DQS_DN is falling and DQS_DP is rising.
6. This value specifies the parameter after write leveling, representing the residual error in the controller after training, and does not include any effects from the DRAM itself.
7. 5200 and 5600 timings apply to 5th Gen Intel® Xeon® Processor Scalable Family.

Figure 6. Command / Control and Clock Timing Waveform

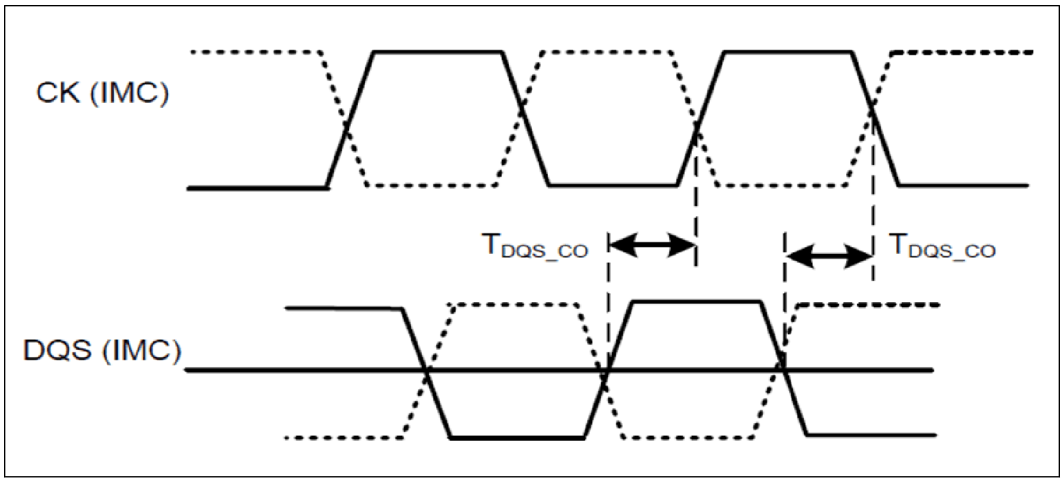
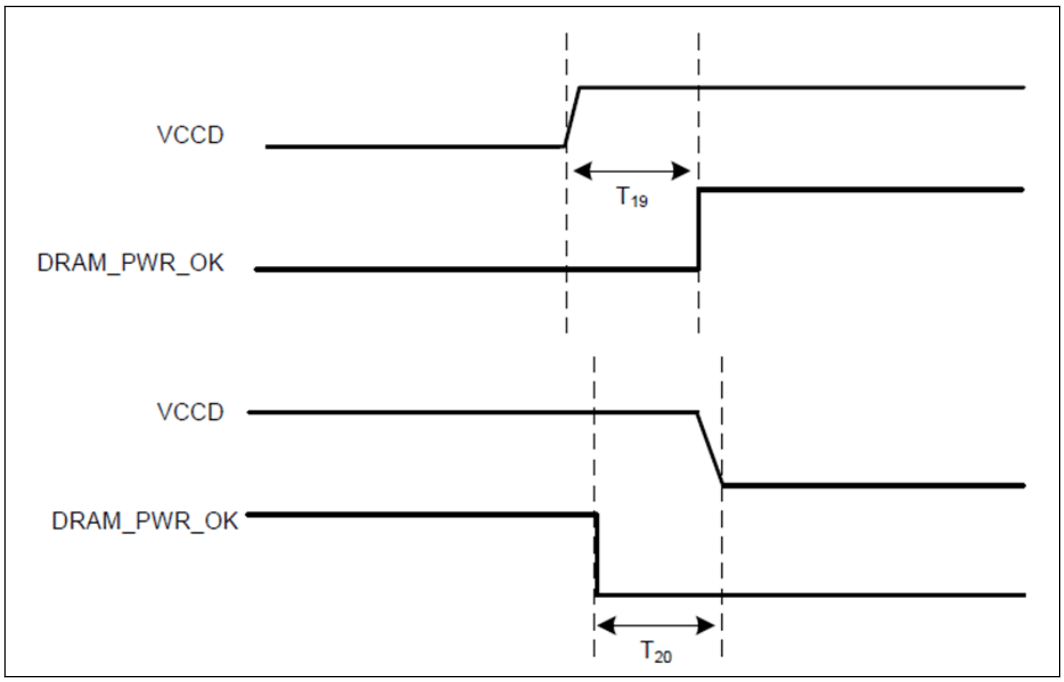


Table 15. DDR5 Miscellaneous Signals AC Specifications

Symbol	Parameter	Min.	Nom.	Max.	Unit	Figure	Note
T19	DDR{01/23/45/67}_DRAM_PWR_OK assertion after VCCDassertion.		0		ms		
T20	DDR{01/23/45/67}_DRAM_PWR_OK de-assertion before VCCDde- assertion.		1		us		

Figure 7. DRAM_PWR_OK Assertion/De-assertion to VCCD Assertion/De-assertion



2.8.2 I3C SPD

Intel's Archer City platform relies on a specialized I3C bus for SPD transactions involving the DDR5 and DDRT2 memory modules. Various industry specifications cover the electrical definitions of such an I3C bus, its controller devices (such as the CPU or BMC), and its connected Target and Hub devices. This section will attempt to summarize the electrical definitions and provide relevant context for OEMs, system designers, FW/SW developers and other interested parties.

Industry Standards:

MIPI I3C Basic* Specification ("**MIPI I3C Basic**")

- Published by: MIPI Alliance Location: https://resources.mipi.org/MIPI-I3C-BASIC-DOWNLOAD, version: 1.1.1 or newer, March 2022 (latest errata revision Er01 at this time).

JEDEC Module Sideband Bus Specification (**JESD403-1A**)

- Published by: JEDEC. Location: https://www.jedec.org/STANDARDS-DOCUMENTS/DOCS/JESD403-1A, version: December 2021 (no errata known at this time).

JEDEC DDR5 LRDIMM and RDIMM Common Specification (**JESD305**)

- Published by: JEDEC. Location: https://www.jedec.org/STANDARDS-DOCUMENTS/DOCS/JESD305, version: January 2022 (no errata known at this time).

JEDEC PMIC50x0 Power Management IC Specification (**JESD301-1A**)

- Published by: JEDEC Location: https://www.jedec.org/standards-documents/docs/jesd301-1a, version: 1.8, August 2021 (no errata known at this time).

Intel's Contribution to Standards

Throughout the development of the JEDEC and MIPI Alliance standard specifications mentioned here, Intel played a key role in shaping these standards and ensuring that Intel platforms could utilize them, to build a robust ecosystem and ensure memory module interoperability. Intel architects, engineers, designers and validators spent countless hours developing the use cases, working with (and across) the standards organizations to ensure that all technical aspects were covered, and validating that our components and platforms behave as expected in compliance with these standards.

Terminology and Nomenclature

Both MIPI and JEDEC specifications use varied terms to describe the aspects/components of an I3C Bus, in a general sense as well as this specific use case. In many cases these terms are aligned, but in other cases they follow different conventions.

Additionally, legacy versions of the referred MIPI and JEDEC specifications used older terms for devices and related parameters, which have since been deprecated. As the industry moves away from offensive terminology, many specifications have replaced terms such as "Master" and "Slave" with more inclusive terms such as "Controller" and "Target" (respectively) even though these new terms do not change the technical definitions. Readers who are familiar with such deprecated terms should ensure that they have the most recent versions of all referred specifications, to be aware of the changes that are moving through these specifications as well as the broader computing industry.

About the I3C Bus for SPD

The MIPI I3C bus is a two-wire serial clock+data utility bus that enables many use cases and applications. When used in a JEDEC compliant platform with DDR5 and DDRT2 memory modules, the I3C bus carries SPD data as well as monitoring and telemetry data for the memory modules that are connected to the platform. The I3C bus can be controlled (that is, driven) by either the Intel CPU or the BMC, see the platform design guide for details. The DDR5/DDRT2 SPD usage of the I3C bus is generally based on MIPI I3C Basic v1.1.1, but uses a lower-voltage (1.0 V) than typical I3C bus for typical generic I3C use cases (for example, 1.8 V). MIPI I3C Basic spec also defines the electrical parameters for a low-voltage, high-capacitance bus (such as the SPD bus) for specialized use cases. JEDEC JESD403-1A uses these low-voltage parameters, but also has specific requirements for this use case, and more precisely defines the electrical parameters and characteristics of such an I3C bus when used with DDR5 and DDRT2 memory modules. As such, platform designers should consult the MIPI I3C Basic Specification to understand the general requirements, and the JEDEC Specifications (such as JESD403-1A) to understand the more specific requirements for an SPD bus.

Intel CPUs that support DDR5 memory modules will include I3C interfaces (that is, GPIOs) that have an I3C Bus Controller instance which can configure the I3C bus, enumerate its target devices, and drive transactions to/from the memory modules for this use case. Such I3C bus controller instances will be configured to operate according to the lower 1.0V parameters, rather than typical generic I3C Bus use cases. Additionally, such I3C bus controller instances will use more specific JEDEC-defined timing parameters that comply with the referred JEDEC specifications for SPD.

As such, the electrical and timing parameters will need to conform to the JEDEC definitions, so that I3C transfers can pass through each memory module's SPD Hub to the other downstream components on the memory module, as defined by JESD403-1A. Each memory module uses an SPD Hub as a bridge between the "Host" side I3C bus segment (that is, between the Controller and Hub) and the "Local" side I3C bus segment (that is, between the Hub and other downstream components on the memory module). Typical I3C buses use the acronyms "SCL" for the serial clock line, and "SDA" for the serial data line. However, JEDEC specifications typically refer to these lines differently based on the I3C bus segment, with "HSCL" and "HSDA" describing the "Host" or upstream segment (that is, from Controller to SPD Hub) and "LSCL" and "LSDA" describing the "Local" or downstream segment (that is, from SPD Hub to other memory module components).

Since the MIPI I3C Basic specification does not cover the SPD Hub or its role as a bridge for downstream components on a memory module, it is common to consider that "SCL" and "SDA" as defined in the MIPI I3C Basic specification are equivalent to "HSCL" and "HSDA" respectively in the JEDEC specifications. However, these downstream components are also I3C Devices and they must also conform to MIPI I3C protocol, although with JEDEC-defined timing and electrical parameters, per JESD403-1A. It is also important to understand that the SPD Hub acts primarily as a level shifter between the upstream and downstream I3C Bus segments, but adds a small internal delay for signal propagation from Host to Local and vice versa. Accordingly, I3C transactions that are driven by the I3C Bus Controller (for example, within Intel CPU) must use timing parameters that allow for such propagation delays across the SPD Hub. With correct timing parameters, the downstream I3C Targets on the DDR5/DDRT2 memory module will able to successfully obtain the clock on "LSDA" and drive "LSDA" for read transfers, while still observing the setup time and hold time requirements for I3C.

Pull-Ups and I3C Operating Modes

I3C devices use both Open Drain mode and Push-Pull mode at various times during I3C transfers. The SDA line has a weak pull-up (called a High-Keeper) that prevents instability and ensures that the line stays high when it is not being driven low. The High-Keeper can also pull SDA to high (relatively slowly) when no other I3C devices are driving it low. In Open Drain mode, the bus controller also conditionally engages a stronger "Open Drain class" pull-up structure, to ensure that SDA returns to high when no other I3C devices are actively driving it low. Open Drain mode allows one or more I3C devices to pull SDA to low at certain times (that is, against the controller's Open Drain class pull-up). If no such I3C devices pull SDA to low, or if an I3C device "lets go" of SDA while it is low, then SDA returns to high (relatively quickly). If SDA was already high when an I3C device "lets go", then SDA stays at high.

In Push-Pull mode, the bus works differently: the controller disengages its Open Drain class pull-up, and only one I3C device is allowed to drive SDA, using active drive for all transitions (that is, to low or to high).

- If the controller is receiving data from an I3C target (that is, for a read transfer), the controller does not act on SDA, and the I3C target that is addressed by the read transfer will actively drive SDA to low or high to send data bits, according to the clock signal that it receives on SCL.

- If the controller is sending data to an I3C target (that is, for a write transfer), the controller actively drives SDA to low or high to send data bits, according to its own clock signal that it sends on SCL. The I3C target that is addressed by the write transfer will receive data but not act on SDA, and all other I3C targets will disengage and wait for a subsequent transfer or command.

I3C sends data in 8-bit intervals followed by a 9th bit, which is called a "T-Bit". During read transfers, the addressed I3C target that provides read data will use the T-bit to indicate whether it has more data bytes to send, which also allows the controller to terminate the read transfer if needed. The SDA line transitions from Push-Pull mode back to Open Drain mode for T-Bits in a read transfer, and then returns to Push-Pull for the next 8 bits of data. During write transfers, the I3C controller uses the T-bit to send a parity bit for each data byte that precedes it, and the I3C target verifies each data byte with the parity bit. In this manner, the controller keeps the SDA line in Push-Pull mode for the 8 bits of data as well as the T-Bit.

By contrast, the SCL line is always driven by the I3C Controller, using Push-Pull timing requirements. The I3C controller chooses the duty cycle and the effective clock frequency, by varying the time spent at high and low. I3C targets on an SPD bus are not permitted to drive the SCL line.

Signaling in Open Drain mode is considerably slower than Push-Pull mode, since the Controller has engaged its Open Drain class pull-up and actively expects other I3C targets to act on the SDA line. In Open Drain mode, I3C targets can pull SDA to low at certain times, in order to gain attention, arbitrate their assigned address at the beginning of a transaction, or otherwise accept a command that is initiated by the controller. By contrast, in Push-Pull mode only one I3C device will drive the SDA line.

NOTE

The previous text applies to SDR (Single Data Rate) mode, as defined by the MIPI I3C Basic Specification. SDR Mode is the default mode of an I3C bus, and all I3C devices are required to support SDR Mode. However, I3C buses can optionally use HDR (High Data Rate) Modes which may use different signaling and can have other requirements that do not apply to SDR Mode, and in some cases these can be quite different from SDR Mode. Some of the statements above will have special exceptions when certain HDR Modes are used. However, the JEDEC specifications for DDR5 SPD buses do not currently allow for HDR Modes since the use case does not currently support any HDR Modes. Furthermore, on Archer City platform architecture all devices should function on I2C FM/FM+ or I3C SDR, there is no support for mix mode transactions, HDR transfers or hot-join.

All I3C Devices that conform to the MIPI I3C specifications will observe these requirements, and will know when to act in either Open Drain mode or Push-Pull mode.

2.8.3 System Reference Clock (BCLK {0/1/2/3}) AC Specifications

Parameter	Signal	Min.	Nominal	Max.	Unit	Figure	Notes$_1$
Reference Clock Frequency	Differential	99.99	100	100.01	MHz		2, 7
BCLK Period	Differential	9.849	10	10.201	ns		2, 7

continued...

Parameter	Signal	Min.	Nominal	Max.	Unit	Figure	Notes[1]
BCLK Edge Rate	Differential	0.6		4	V/ns	Figure 8	4, 7, 8
BCLK Dutycycle	Differential	45		55	%	hFigure 9	7
BCLK cycle to cycle jitter	Differential			|100|	ps		3, 7
VRB	Differential	-100		100	mV	Figure 10	5, 7
TStable	Differential	500			ps		6, 7

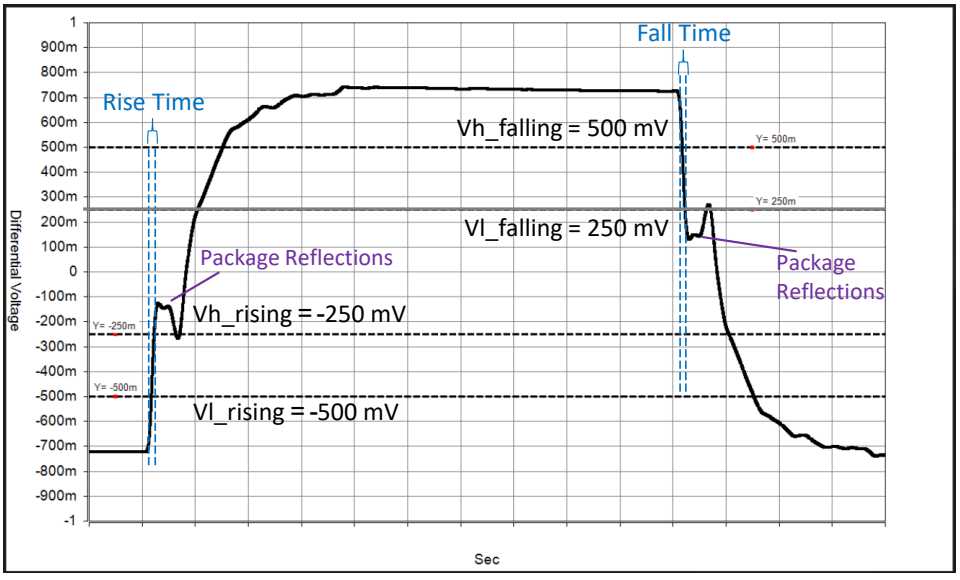
Notes:

1. Unless otherwise noted, all specifications in this table apply to all processor frequencies.
2. Average Period.
3. This is absolute cycle to cycle jitter.
4. Edge Rate (V/ns) is calculated as 250 mV divided by the rise or fall times measured using the thresholds in Figure 8.
5. Measurement taken from differential waveform.
6. TStable is the time the differential clock must maintain a minimum ±150 mV differential voltage after rising/falling edges, before it is allowed to droop back into the VRB ±100 mV range. See Figure 10 on page 48.
7. Specifications can be validated at the pin.
8. Measured with a CPU in the socket to get die loading effects. Sapphire Rapids XCC provides maximum loading for min spec measurement.

NOTE

Refer to PCI Express* Base Specification Revision 5.0 for additional PCIe compliance requirements like Spread Spectrum Clocking, PPM, RMS Phase Jitter, low frequency jitter, Rise-Fall Matching, and so forth.

Figure 8. BCLK{0/1/2/3} Differential Clock Measurement Points for Edge Rate



The previous figure provides the thresholds needed to verify the edge rate specifications. It also shows an example of what package reflections might look like when measuring with a CPU in place. However, it is not an exact reference and is not intended to be compared with measurement data.

Figure 9. BCLK{0/1/2/3} Differential Clock Measurement Points for Duty Cycle and Period

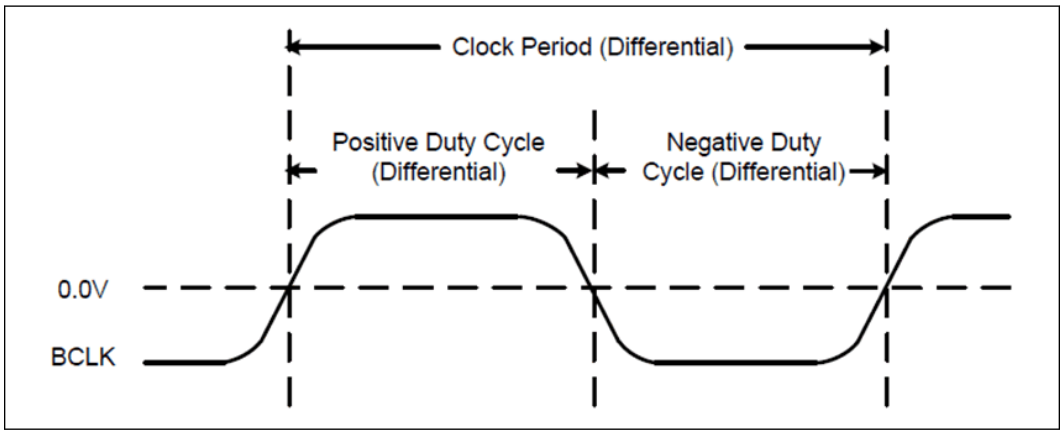
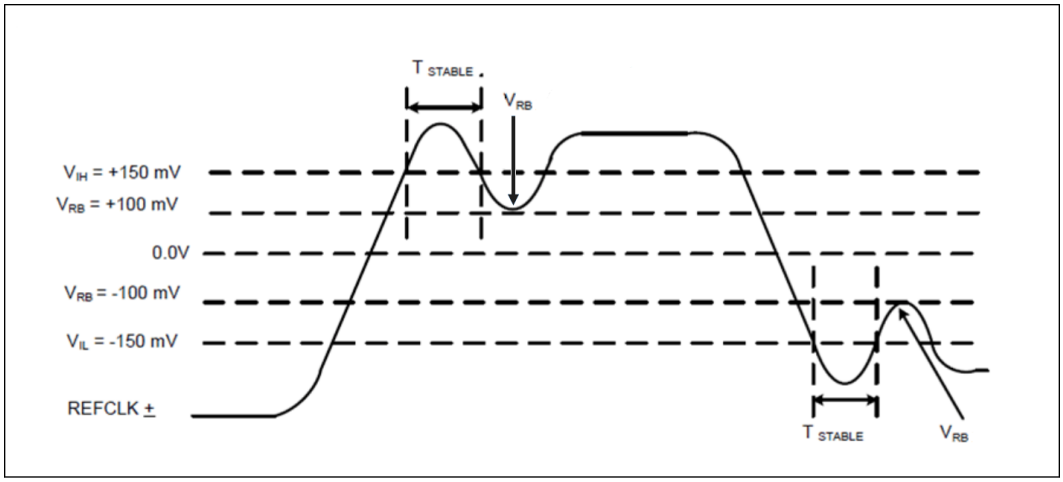


Figure 10. BCLK{0/1/2/3} Differential Clock Measurement Point for Ringback



2.8.4 XTAL_CLK AC Specifications

Table 16. XTAL_CLK AC Specifications

Parameter	Signal	Min.	Nominal	Max.	Unit	Figure	Notes
XTAL_CLK Clock Frequency	Differential	24.9975	25	25.0025	MHz		2, 7, 8
XTAL_CLK Period	Differential	39.996	40	40.004	ns		2, 7, 8
XTAL_CLK Edge Rate	Differential	1.0		4.0	V/ns	Figure 8	4, 7, 9, 10

continued...

Parameter	Signal	Min.	Nominal	Max.	Unit	Figure	Notes
XTAL_CLK Dutycycle	Differential	45		55	%	Figure 9	7, 9
XTAL_CLK cycle to cycle jitter	Differential			|1.3|	ns		3, 7
VRB	Differential	-100		100	mV	Figure 10	5, 7, 9
TStable	Differential	500			ps		6, 7, 9

Notes:

1. Unless otherwise noted, all specifications in this table apply to all processor frequencies.
2. Average Period.
3. This is absolute cycle to cycle jitter.
4. Edge Rate (V/ns) is calculated as 250 mV divided by the rise or fall times measured using the thresholds in Figure 8.
5. Measurement Taken from differential waveform.
6. TStable is the time the differential clock must maintain a minimum ±150 mV differential voltage after rising/falling edges, before it is allowed to droop back into the VRB ±100 mV range. See Figure 10.
7. Specifications can be validated at the pin.
8. XTAL_CLK does not support spread spectrum clocking (SSC). Measure with a frequency counter.
9. BCLK Figures are applicable to XTAL_CLK.
10. Measured with a CPU in the socket to get loading effects from multiple dice. Sapphire Rapids XCC provides maximum loading for min spec measurement. The dice bumps require edge rates of 0.4 V/ns minimum and 4.0 V/ns maximum.

2.8.5 SMBus Signal AC Specifications

		Standard-Mode		Fast-Mode		Fast-Mode Plus				
Symbol	Parameter	Min.	Max.	Min.	Max.	Min.	Max.	Unit	Figure	Notes[1, 2]
Transmitter and Receiver Timings										
FSMB	SMBCLK Frequency.	10	100	10	400	10	1000	kHz	Figure 11 on page 50	3
tLOW	LOW period of the SMB clock.	4.7		1.3		0.5		µs		3
tHIGH	HIGH period of the SMB clock.	4.0		0.6		0.26		µs		
tSU;DAT	Data Setup Time.	250		100		50		ns		
tHD;DAT	Data Hold Time.	0		0		0		µs		
tHD;STA	Hold Time after (Repeated) Start Condition.	4.0		0.6		0.26		µs		
tSU;STA	Repeated Start Condition Setup Time.	4.7		0.6		0.26		µs		
tSU;STO	Stop Condition Setup Time.	4.0		0.6		0.26		µs		
T5	SMBus Output Valid Delay.		3.45		0.9		0.45	µs	Figure 12 on page 50	4
tBUF	Bus Free time between STOP and START conditions	4.7		1.3		0.5		µs		

continued...

		Standard-Mode		Fast-Mode		Fast-Mode Plus				
Symbol	**Parameter**	**Min.**	**Max.**	**Min.**	**Max.**	**Min.**	**Max.**	**Unit**	**Figure**	**Notes[1, 2]**
tF	Clock/Data Fall Time		300		300		120	ns		
tR	Clock/Data RiseTime		1000		300		120	ns		

Notes:
1. These parameters are based on design characterization and are not tested.
2. All AC timings for the SMBus signals are referenced at VIL_MAX or VIH_MIN and measured at the processor pins. See Figure 11 on page 50.
3. These parameters might change depending on optimized value found for multi-slave configurations.
4. If connected device supports FS or FS+ mode, you can refer to voltage/timing specs for device max supported speed.

Figure 11. SMBus Timing Waveform

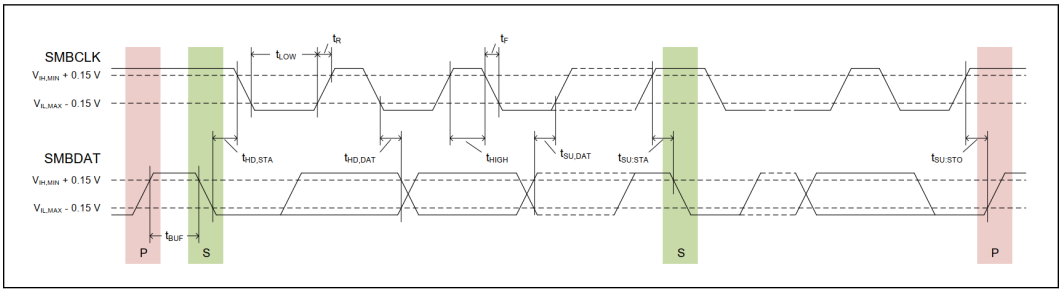
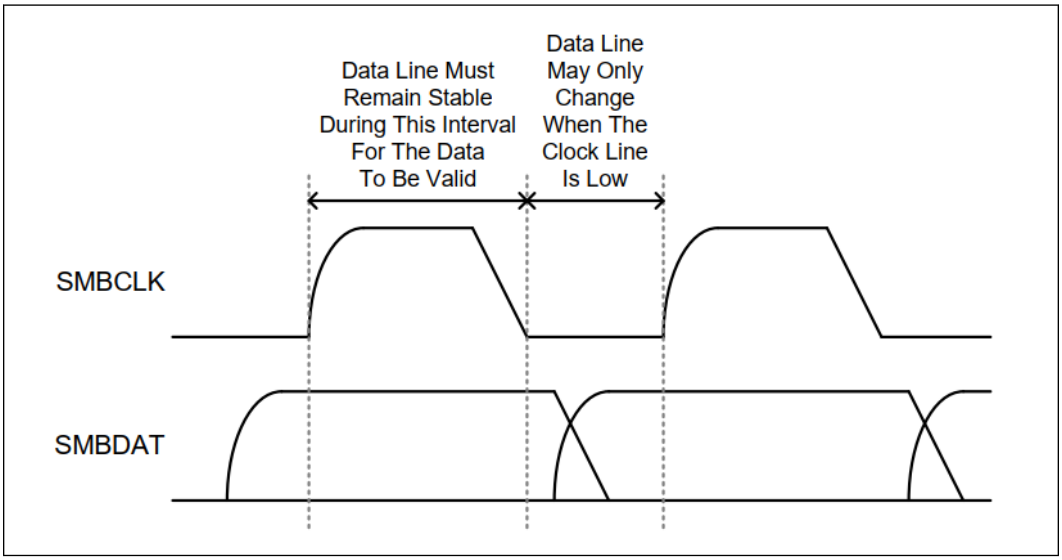


Figure 12. SMBus Valid Delay Timing Waveform



2.8.6 JTAG and TAP Signal AC Specifications

T# Parameter	Min.	Max.	Unit	Figure	Notes[1, 2]
TCK Frequency.		100	MHz		
TCK Output Pulse Width.	5		ns	Figure 13 on page 51	

continued...

T# Parameter	Min.	Max.	Unit	Figure	Notes[1, 2]
T1,T2: TDI, TDO, TMS Pulse Width.	1		TCK		
T1,T2: TCKs required.	2		TCK		
T1,T2: BPM_N[7:0] Input Pulse Width.	5		ns		
T1,T2: BPM_N[7:0] Output Pulse Width.	10		ns		
T3, T4: PREQ_N Rise/Fall Time (VIL to VIH).		15	ns		
T5: BCLK0 to BPM_N [7:0] Output Valid Delay.	1	8.6	ns	Figure 14 on page 52	
T5: BCLK0 to PRDY_N Output Valid Delay.	N/A	5	ns		
T5: TCK to TDO Output Valid Delay.		5	ns		4
Ts: TDI, TMS Setup Time.	6.5		ns	Figure 15 on page 52	3
Th: TDI, TMS Hold Time.	6.5		ns		3
Boundary scan all non test input setup (PREQ_N).	15		ns		6, 7
Boundary scan all non test input hold (PREQ_N).	15		ns		6, 7

Notes:
1. Unless otherwise noted, all specifications in this table apply to all processor frequencies.
2. Not 100% tested. Specified by design characterization.
3. Referenced to the rising edge of TCK. Assuming minimum edge rate of 0.5 V/ns.
4. Referenced to the falling edge of TCK at the processor pad.
5. Referenced to the falling edge of TCK.
6. Referenced to the rising edge of TCK.

Figure 13. JTAG/Tap and Processor Sideband Signals High/Low Pulse Widths and Rise/Fall Times

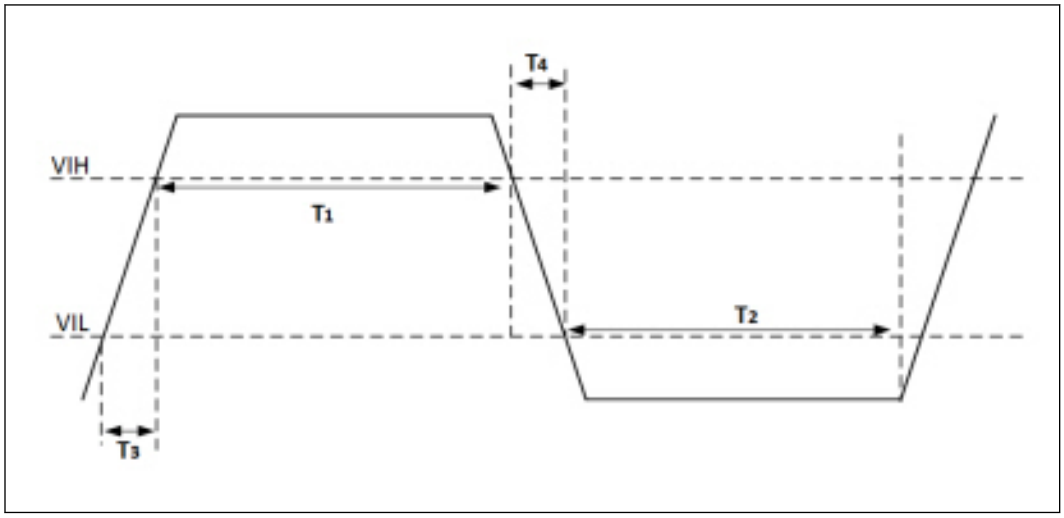


Figure 14. BCLK to JTAG/TAP Signals Output Valid Delays

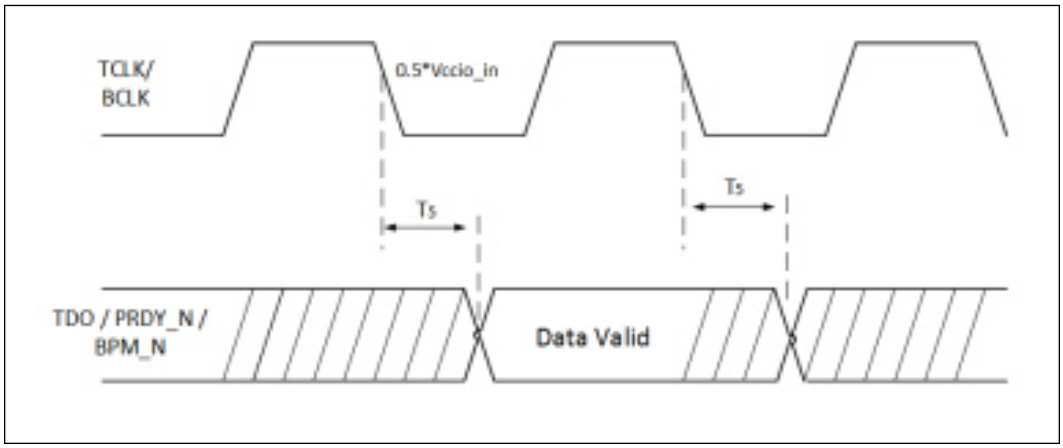
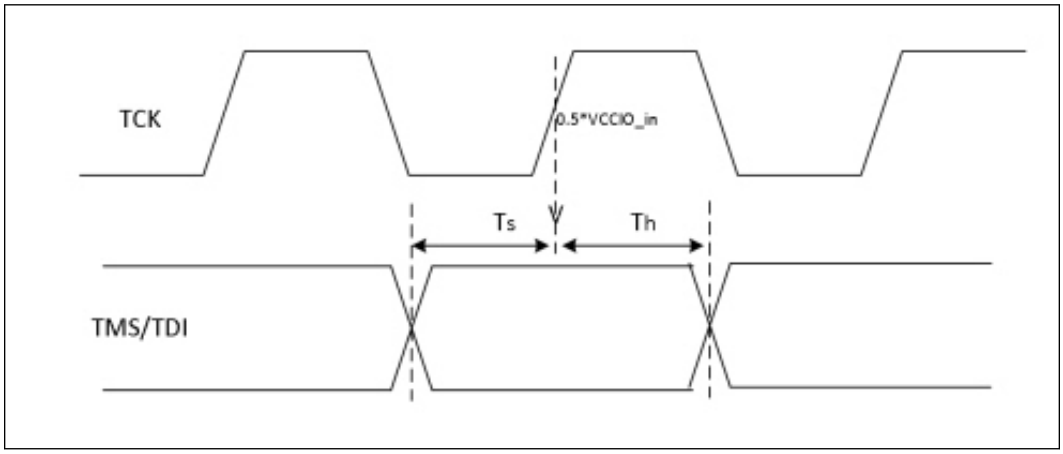


Figure 15. JTAG/TAP Input Valid Delay Timing Waveform



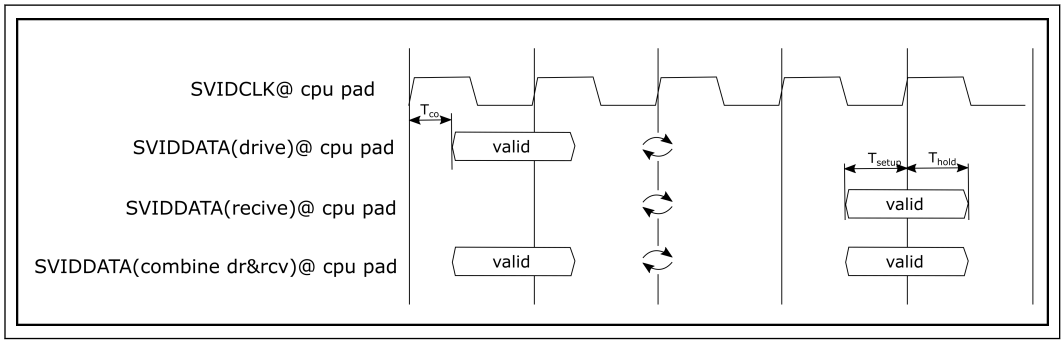
2.8.7 Serial VID (SVID) Interface AC Timing Specifications

Symbol	Parameter	Min.	Nom.	Max.	Units	Figure	Notes
	SVIDCLK Frequency (VCLK).		25		MHz	Figure 16 on page 53	1
TPeriod	Absolute Minimum SVIDCLK Period.	(1/VCLK) - 5%	(1/VCLK)	(1/VCLK) + 5%	ns		1
THigh/Low	SVIDCLK High and Low Time.	(1/VCLK)/2 - 20%	(1/ VCLK)/2	(1/VCLK)/2 + 20%	ns		1, 3, 4
Tco	SVIDDATA Output Delay from SVIDCLK.	-1		1	ns		1, 2, 4
TS	SVIDDATA Input Setup Time.	1			ns		1
TH	SVIDDATA Input Hold Time.	5			ns		1, 2
Notes:							

continued...

Symbol	Parameter	Min.	Nom.	Max.	Units	Figure	Notes
1. Unless otherwise noted, all specifications in this table apply to all processor frequencies. 2. Referenced to the rising edge of SVIDCLK at 0.5×VCCINFAON. 3. THigh is measured with respect to 0.7×VCCINFAON. T_{Low}time is measured with respect to 0.3×VCCINFAON. 4. Value obtained through test bench with 50Ω pull up to VCCINFAON.							

Figure 16. Serial VID Interface (SVID) Signals Clock Timings



2.8.8 Processor Asynchronous Miscellaneous I/O AC Specifications

Parameter	Min.	Max.	Unit	Figure	Notes[1]
T2: PROCHOT_N Input Pulse Width Low.	500		µs	Figure 17 on page 55	
T1: PROCHOT_N Input Pulse Width High.	5		µs		
T2: PROCHOT_N Output Pulse Width Low.	500		µs		
T1: PROCHOT_N Output Pulse Width High.	500		µs		
Ts: PROCHOT_N Setup Time.	1		µs	Figure 18 on page 56	
Th: PROCHOT_N Hold Time.		TBD	µs		
T3: PROCHOT_N Rise Time.		80	ns		10
T4: PROCHOT_N Fall Time.		80	ns		10
T2: RESET_N Input Pulse Width Low.	3.5		ms		
T1: RESET_N Input Pulse Width High.	4		BCLK0		
T3, T4: RESET_N Rise Time (VIL to VIH) / Fall Time (VIH to VIL).		15	ns		
T7: FRB Cold Boot: RESET_N de-assertion to PROCDIS_N de-assertion.	1		µs	Figure 19 on page 57	
T8: FRB Warm Boot: PROCDIS_N assertion to RESET_N assertion.	1		µs		
T9: FRB Warm Boot: RESET_N de-assertion to PROCDIS_N de-assertion.	1		µs		

continued...

Parameter	Min.	Max.	Unit	Figure	Notes[1]
T2: CATERR_N Input Pulse Width Low.	3		BCLK0		6
T1: CATERR_N Input Pulse Width High.	3		BCLK0		
T2: CATERR_N Output Pulse Width Low.	16		BCLK0		
T3: CATERR_N Rise Time.		80	ns		10
T4: CATERR_N Fall Time.		80	ns		10
T10: THERMTRIP_N assertion until VCCIN/VCCINFAON/VCCD removed.		500	ms	Figure 20 on page 58	6
MEM_HOT_C{01/23}_N Output Pulse Width Low and High.	1		DCLK		2, 3
MEM_HOT_C{01/23}_N Input Pulse Width Low.	>MH_SENSE_ PERIOD	<=MH_SENSE_ PERIOD	µs	Figure 21 on page 58	4
T3:MEM_HOT_C{01/23}_N Rise Time.		80	ns	Figure 17 on page 55	10
T4:MEM_HOT_C{01/23}_N Fall Time.		80	ns		10
T3:PWRGOOD Input Signals Rise Time T4:PWRGOOD Input Signals Fall Time.		50	ns		5
T11: BCLK0 stable to PWRGOOD assertion.	10		BCLK0	Table 17 on page 58	
T12: PWRGOOD assertion to RESET_N de-assertion.	3.5		ms		7, 8
T13: TSetup:Power-On Configuration Setup Time to PWRGOOD assertion, Signals: BMCINIT, TXT_PLTEN, FRMAGENT, TXT_AGENT, SAFE_MODE_BOOT, SOCKET_ID[1:0].	1		µs		6
T14: THold:Power-On Configuration Hold Time, Signals: BMCINIT, TXT_PLTEN, FRMAGENT, TXT_AGENT, SAFE_MODE_BOOT, SOCKET_ID[1:0].	TBD		µs		6
T15: VCCINFAON stable to PWRGOOD assertion.	1		ms		
PROCDIS Pulse Width.	50		ns		
PROCDIS Setup Time to PWRGOOD.	0		ns		
PROCDIS Setup Time to RESET_N assertion edge.	0		ns		
PROCDIS Hold Time to PWRGOOD.	10		ms		
PROCID Hold Time to RESET_N assertion edge.	1		ms		
T3: NMI Input Signals Rise Time.		80	ns	Table 17 on page 58	10

NOTES

1. Unless otherwise noted, all specifications in this table apply to all processor frequencies.
2. DCLK is DDR{0/1/2/3/4/5/6/7}_CLK_DN/DP[3:0]. DCLK is relative to the MH_IN_SENSE_ASSERT range, but the whole MEM_HOT_C{012/345}_N output assertion time is based on the MEM_HOT_C{012/345}_N event assertion, Figure 21 on page 58
3. Maximum High pulse width is constant High when there are no MEM_HOT_C{012/345}_N events, and the MH_SENSE_EN=0.
4. MH_SENSE_PERIOD is the MEM_HOT_C{012/345}_N sense period and guarantees external assertion detection, see the *4th Gen Intel® Xeon® Scalable Processor, Codename Sapphire Rapids, Sapphire Rapids EE, Emerald Rapids Processor, or Eagle Stream Platform Register Specification* and the *Eagle Stream Platform BIOS Writer's Guide*. This is the configurable sense period and sense assertion time. When sense assertion time is set to zero, and the processor is asserting MEM_HOT_C{012/345}_N it will ignore externally asserted MEM_HOT_C{01/23}_N.
5. Sense period: 50 µs, 100 µs, 200 µs, or 400 µs. This timing value is the one measured from ViL to ViH.
6. Sense assertion time: 0, 1 µs, 1.5 µs, 2 µs, 2.5 µs, 3 µs, or 3.5 µs.
7. Tpwrgood_fall and Tpwrgood_rise are measured: 0.3×VCCINFAON to 0.7×VCCINFAON.
8. These signals are sampled after PWRGOOD assertion.
9. To meet TSC (Time Stamp Counter) multi-socket sampling, PWRGOOD must arrive to all processors within 1 BCLK{0/1} and the BCLK{0/1} skew between the sockets should be less than one-half (1/2) BCLK{0/1} cycle. For details on platform implementation, see the appropriate Platform Design Guide (PDG).
10. This timing value is the one measured from ViL - 50 mV to ViH + 50 mV.

Figure 17. JTAG/Tap and Processor Sideband Signals High/Low Pulse Widths and Rise/Fall Times

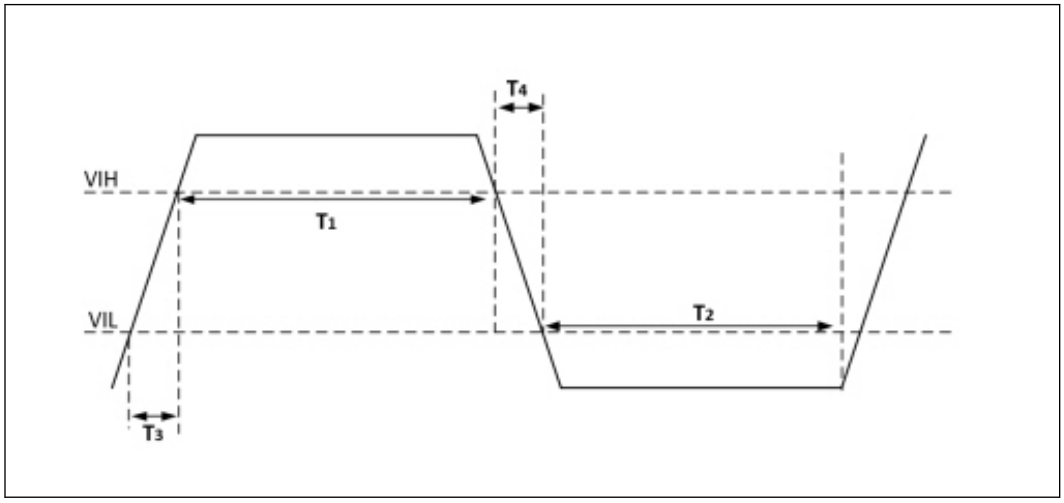


Figure 18. PROCHOT_N Setup and Hold Timing Waveforms

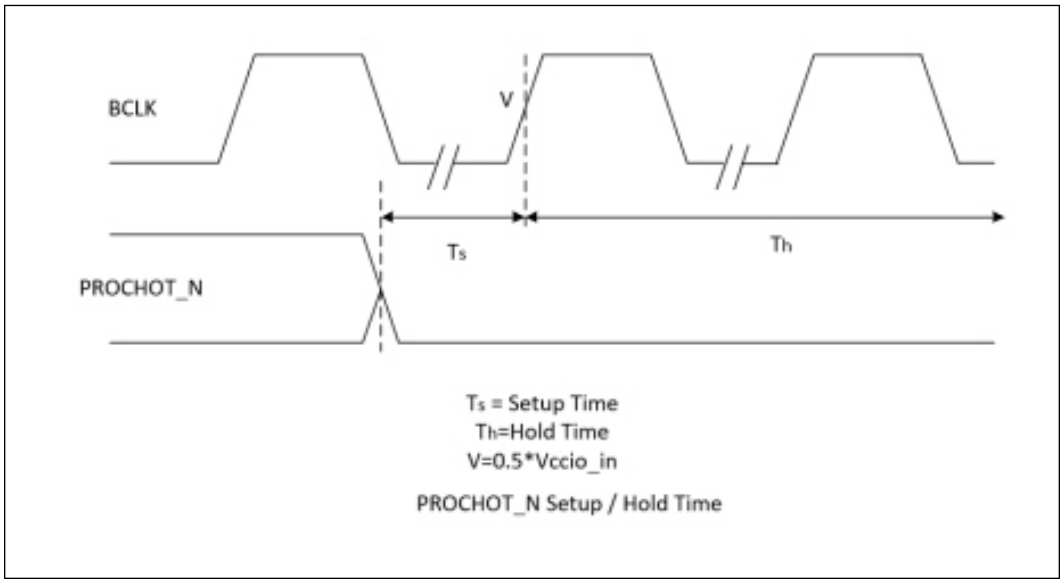


Figure 19. Fault Resilient Booting (FRB) Timing Requirements

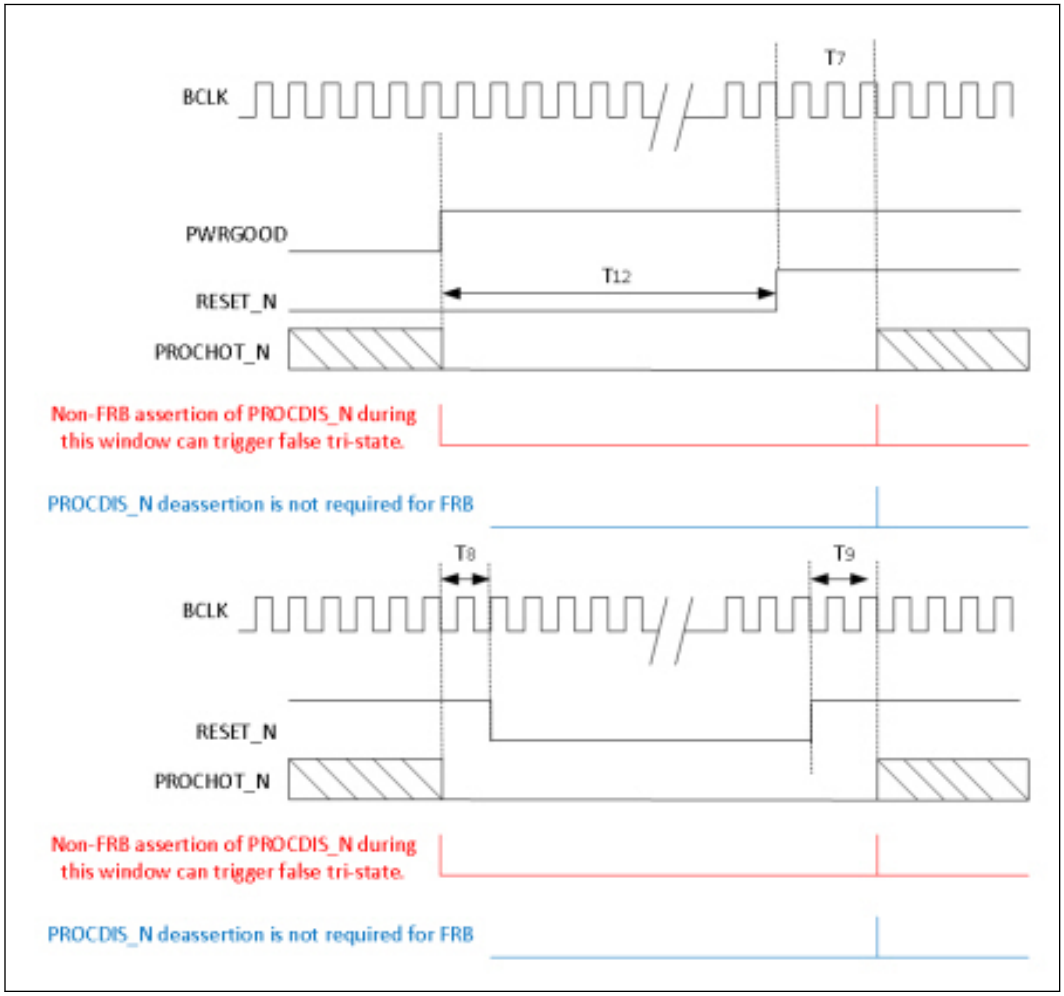


Figure 20. THERMTRIP_N Assertion Until VCCIN, VCCD, VCCVNN and VCCVNN Removal

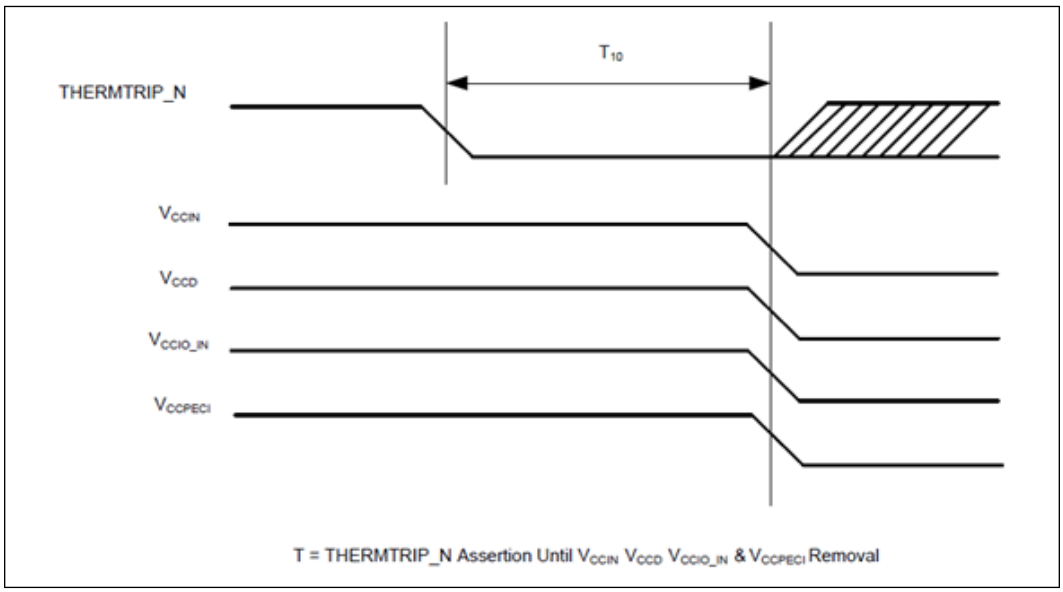
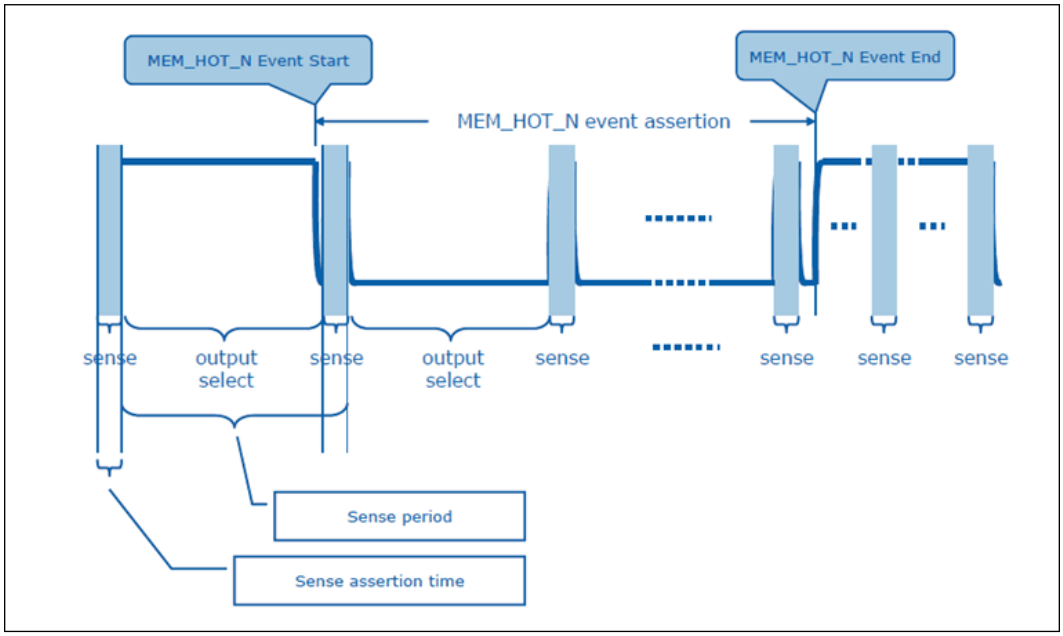


Table 17. Voltage Sequence Timing Requirements

See the *Eagle Stream Platform Design Guide*, document number 610826.

Figure 21. MEM_HOT_C{012/345}_N Event Assertion Waveform



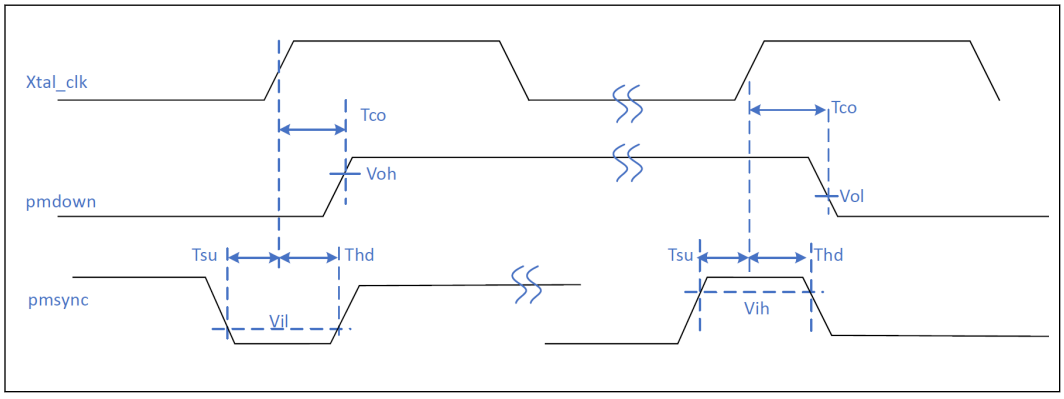
2.8.9 SBLINK AC Specifications

This section describes the DC Specifications for the SBLINK.

Symbol	Parameter	Min.	Max.	Units	Figure	Notes[2]
Tco	CLK to Data Delay PMDOWN_PCH	7.32	23.41	ns		1
	CLK to Data Delay PMDOWN[6:0] (1S/2S CPU)	7.32	23.41	ns		1,3
	CLK to Data Delay PMDOWN[6:0](4S/8S CPU)	5.00	15.70	ns		1,4
Tsu	Setup Time PMSYNC[6:0]/ PMSYNC_PCH	1.86	-	ns		1
Thd	Hold Time PMSYNC[6:0]/ PMSYNC_PCH	2.19	-	ns		1
Input SR	Slew Rate PMSYNC[6:0]/ PMSYNC_PCH	40	1000	mV/ns		5

Notes:
1. The XTAL_CLK measurement threshold should be 150 mV on rising edge of the differential waveform.
2. Unless otherwise noted, all specifications in this table apply to all processor frequencies.
3. Timing applies to CPU QDFs/S-Specs that only support one and two socket operation.
4. Timing applies to CPU QDFs/S-Specs that support four or greater socket operation.
5. Parameter to be measured between VIL-VIH.

Figure 22. SBLINK Setup and Hold timing Waveforms



2.9 Package C-State Power Specifications

The table below lists the processor package C-state power specifications for the various processor SKUs.

Die Type	C6 (W)
XCC	65
MCC	45
HBM	80

Notes:
1. SKUs are subject to change. Contact your Intel Field Representative to obtain the latest SKU information.
2. Package C6 power specified at T_{CASE} = 50°C.

2.10 Signal Quality

Data transfer requires the clean reception of data signals and clock signals. Ringing below receiver thresholds, non-monotonic signal edges, and excessive voltage swings will adversely affect system timings. Ringback and signal non-monotonicity cannot be tolerated since these phenomena may inadvertently advance receiver state machines. Excessive signal swings (overshoot and undershoot) are detrimental to silicon gate oxide integrity, and can cause device failure if absolute voltage limits are exceeded.

Overshoot and undershoot can also cause timing degradation due to the build up of Inter-Symbol Interference (ISI) effects.

For these reasons, it is crucial that the designer work towards a solution that provides acceptable signal quality across all systematic variations encountered in volume manufacturing.

This section documents signal quality metrics used to derive topology and routing guidelines through simulation. All specifications are specified at the processor die (pad measurements).

Specifications for signal quality are for measurements at the processor core only and are only observable through simulation. Therefore, proper simulation is the only way to verify proper timing and signal quality.

2.10.1 DDR Signal Quality Specifications

Various scenarios for the DDR Signals have been simulated to generate a set of layout guidelines.

Overshoot (or undershoot) is the absolute value of the maximum voltage above or below VSS. The overshoot/undershoot specifications limit transitions beyond specified maximum voltages or VSS due to the fast signal edge rates. The processor can be damaged by single and/or repeated overshoot or undershoot events on any input, output, or I/O buffer if the charge is large enough (that is, if the over/undershoot is great enough). Baseboard designs which meet signal integrity and timing requirements and which do not exceed the maximum overshoot or undershoot limits listed in Table 18 on page 61 will ensure reliable IO performance for the lifetime of the processor.

2.10.2 PCIe Signal Quality Specifications

Signal Quality specifications for PCIe Signals are included as part of the PCIe DC specifications and PCIe AC specifications. Various scenarios have been simulated to generate a set of layout guidelines.

2.10.3 Intel UPI Signal Quality Specifications

Signal Quality specifications for Differential Intel® UPI Signals are included as part of the Intel® UPI defined in the Intel® UPI specifications. Various scenarios have been simulated to generate a set of layout guidelines.

2.10.4 Input Reference Clock Signal Quality Specifications

Overshoot/Undershoot and Ringback specifications for BCLK{0/1/2/3}_D[N/P] are found in Table 18 on page 61. Overshoot/Undershoot and Ringback specifications for the DDR5 Reference Clocks are specified by the DIMM manufacturer.

2.10.5 Overshoot/Undershoot Tolerance

Overshoot (or undershoot) is the absolute value of the maximum voltage above or below VSS, see Figure 23 on page 62. The overshoot/undershoot specifications limit transitions beyond VCCD or VSS due to the fast signal edge rates. The processor can be damaged by single and/or repeated overshoot or undershoot events on any input, output, or I/O buffer if the charge is large enough (that is, if the over/undershoot is great enough). Baseboard designs which meet signal integrity and timing requirements and which do not exceed the maximum overshoot or undershoot limits listed in the following table will insure reliable IO performance for the lifetime of the processor.

Table 18. Processor I/O Overshoot/Undershoot Specifications

Signal Group	Maximum Undershoot	Maximum Overshoot	Overshoot Duration	Undershoot Duration	Notes
DDR5	-0.22×VCCD	1.22×VCCD	0.25×TCH	0.1×TCH	1,2,3,5
Processor Asynchronous Sideband Signals, SVID, miscellaneous and JTAG/Tap Signals	-0.35×VCCINFAON	1.35×VCCINFAON	1.25 ns	0.5 ns	1,2,5
System Reference Clock (BCLK{0/1/2/3})	-0.15V	1.15V	N/A	N/A	1,2,5
PWRGOOD Signal	-0.42V	VCCINFAON + 0.28 V	5 ns	5 ns	1,2,4
PMSYNC[6:0] Signals	-0.35×VCCINFAON	1.35×VCCINFAON	5 ns	5 ns	1,2
PECI Signal	-0.35V	1.35V	5 ns	5 ns	1,2
SVIDDATA Signal	-0.3V	1.3V	10 ns	10 ns	1,2

Notes:

1. These specifications are computer simulated at the processor pad (inside the CPU package).
2. Refer to Figure 23 on page 62 for description of allowable Overshoot/Undershoot magnitude and duration.
3. TCH is the minimum high pulse width duration, see DDR5 Signals AC Specifications on page 41 for details on DDR5 TCH.
4. For PWRGOOD DC specifications see Processor Asynchronous Miscellaneous I/O DC Specifications on page 39.
5. Refer to Table 8 on page 20 for a list of signals under the different signal groups, except for the signals that are explicitly listed on this table.

2.10.5.1 Overshoot/Undershoot Magnitude

Magnitude describes the maximum potential difference between a signal and its voltage reference level. For the processor, both are referenced to VSS. It is important to note that the overshoot and undershoot conditions are separate and their impact must be determined independently.

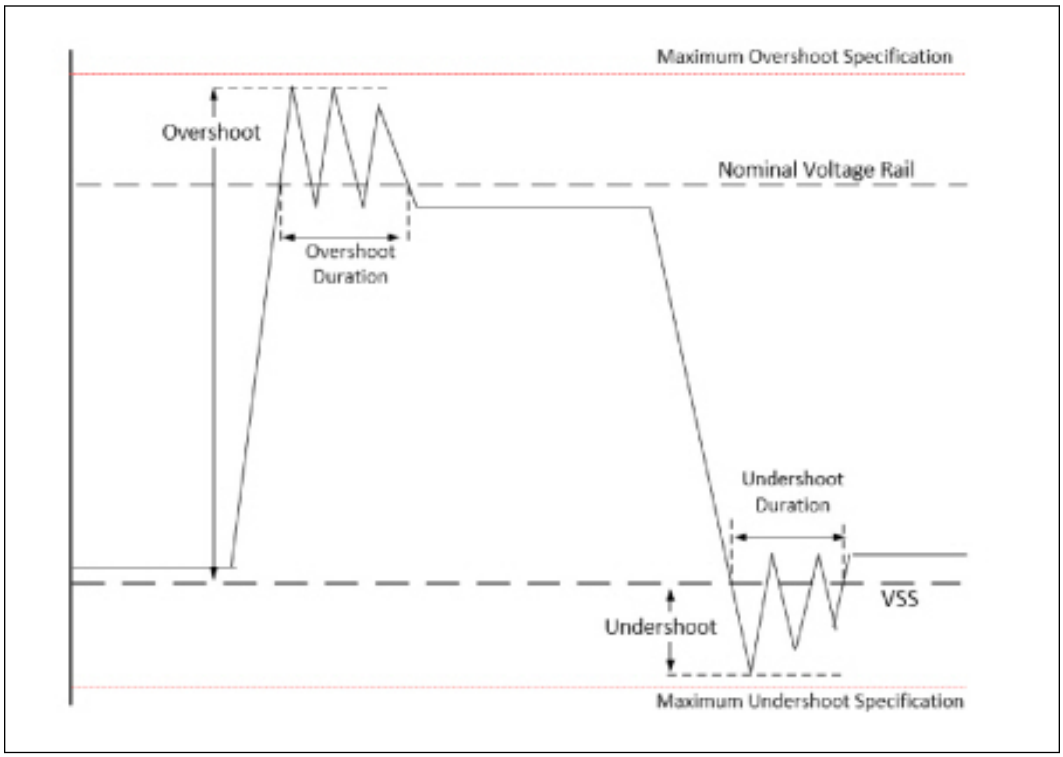
2.10.5.2 Overshoot/Undershoot Pulse Duration

Pulse duration describes the total amount of time that an overshoot/undershoot event exceeds the overshoot/undershoot reference voltage. The total time could encompass several oscillations above the reference voltage. Multiple overshoot/undershoot pulses within a single overshoot/undershoot event may need to be measured to determine the total pulse duration.

NOTE

Oscillations below the reference voltage cannot be subtract the total overshoot/ undershoot pulse duration.

Figure 23. Maximum Acceptable Overshoot/Undershoot Waveform



2.10.5.3 Reading Overshoot/Undershoot Specification Tables

The overshoot/undershoot specification for the processor is not a simple single value. Instead, many factors are needed to determine the over/undershoot specification. In addition to the magnitude of the overshoot the width of the overshoot is needed. To determine the allowed overshoot for a particular overshoot event, the following must be done:

1. Determine the signal group a particular signal falls into.
2. Determine the magnitude of the overshoot or the undershoot.
3. Determine the duration of the undershoot or the overshoot.
4. Compare the values obtained with the maximum overshoot/undershoot magnitude, if this value exceeds the nominal voltage rail, then the duration should be measured, if this value surpasses the maximum overshoot/undershoot duration then this case is a violation.

Undershoot events must be analyzed separately from overshoot events as they are mutually exclusive.

2.10.5.4 Determining if a System Meets the Overshoot/Undershoot Specifications

The overshoot/undershoot specifications listed in the table specify the allowable overshoot/undershoot for a single overshoot/undershoot event. However, most signals will have multiple overshoot and/or undershoot events that each have their own set of parameters (duration and magnitude). To ensure a signal passes the overshoot and undershoot specifications, measure the worst case magnitude and compare it against the maximum allowed overshoot/undershoot value.

3.0 Signal Descriptions

This chapter describes the Intel® Xeon® processor Scalable Family signals. They are arranged in functional groups according to their associated interface or category.

3.1 System Memory Interface

Table 19. Memory Channel DDR0, DDR1, DDR2, DDR3, DDR4, DDR5, DDR6, DDR7

Signal Name	Description
DDR[7:0]_CLK[1:0]	Differential Clocks for each channel.
DDR[7:0]_SA_CS[1:0], DDR[7:0]_SB_CS[1:0], DDR[7:0]_SA_CS[3:2], DDR[7:0]_SB_CS[3:2]	For standard DIMMs there are Chip selects, one per device electrical rank (OR per 3DS stack for 3DS RDIMMs) for SA and SB. For DDR-T2 these signals are used for Chip function and/or training functions.
DDR[7:0]_SA_DQ[31:0] DDR[7:0]_SB_DQ[31:0]	Data buses for Sub-channel A (SA) and Sub-channel B (SB) per channel.
DDR[7:0]_SA_DQS[9:0] DDR[7:0]_SB_DQS[9:0]	Differential data strobes for Sub-channels SA and SB.
DDR[7:0]_SA_ECC[7:0] DDR[7:0]_SB_ECC[7:0]	For standard DIMMs these are ECC check bits for SA and SB. For DDR-T2 these are a combination of ECC and metadata bits.
DDR[7:0]_SA_CA[6:0], DDR[7:0]_SB_CA[6:0]	Command and Address for SA and SB.
DDR[7:0]_SA_PAR, DDR[7:0]_SB_PAR	Command and Address parity for SA and SB.

Table 20. Memory Channel Miscellaneous

Signal Name	Description
DDR{01/23/45/67}_RESET_N	System memory reset per IMC: Reset signal from processor to DRAM devices on the DIMM. For DDR-T2 DIMMs the signal resets the DDR-T2 interface, but not the Far Memory Controller.
DDR[0123/4567]_SPDSCL DDR[0123/4567]_SPDSDA	Used for interfacing to the DIMM Serial Presence Detect (SPD) for each DIMM. DDR[0123/4567]SPD_SCL Two sets of interfaces per processor.
DDR[7:0]_ALERT_N	Indicates Parity Error or CRC detected by DIMM per channel. Currently not used for DDR-T2 protocol.
DDR[01/23/45/67]_DRAM_PWR_OK	DIMM power status for each IMC.
DDR[7:0]_A_RSP[1,0] DDR[7:0]_B_RSP[1,0]	DIMM Response signals for each channel. For DDR-T2 DDR[7:0]_A/B_RSP[1,0] are the REQ# signal and ERR# signals, respectively. They are shared by both sub-channels.

3.2 PCI Express Based Interface Signals

NOTE

PCI Express Ports 0, 1, 2, 3, and 4 Signals are receive and transmit differential pairs.

Table 21. PCI Express Signals

Signal Name	Description
PE{4:0}_RX_DN/DP[15:0]	PCIe Receive Data Input
PE{4:0}_TX_DN/DP[15:0]	PCIe Transmit Data Output

Table 22. PCI Express Miscellaneous Signals

Signal Name	Description
CXPSMBUSSCL	PCI Express Hot-Plug SMBus Clock: Provides PCI Express HOT PLUG* support via a dedicated SMBus interface. Requires an external general purpose input/output (GPIO) expansion device on the platform.
CXPSMBUSSDA	PCI Express Hot-Plug SMBus Data: Provides PCI Express HOT PLUG support via a dedicated SMBus interface. Requires an external general purpose input/output (GPIO) expansion device on the platform.
CXPSMBUS_ALERT_N	PCI Express Hot-Plug SMBus Alert: Provides PCI Express HOT PLUG support via a dedicated SMBus interface. Requires an external general purpose input/output (GPIO) expansion device on the platform.

3.3 DMI3 Signals

Table 23. DMI3 Signals

Signal Name	Description
DMI_RX_DN/DP[7:0]	DMI3 Receive Data Input
DMI_TX_DN/DP[7:0]	DMI3 Transmit Data Output

3.4 Intel UPI Signals

Table 24. Intel® UPI Signals

Signal Name	Description
UPI{3:0}_RX_DN/DP[23:0]	Intel® UPI Receive data input.
UPI{3:0}_TX_DN/DP[23:0]	Intel® UPI Transmit data output.

3.5 PECI Signal

Table 25. PECI Signal

Signal Name	Description
PECI	Platform Environment Control Interface (PECI) is the serial sideband interface to the processor and is used primarily for thermal, power and error management.

3.6 System Reference Clock Signals

Table 26. System Reference Clock (BCLK{0/1/2/3}) Signals

Signal Name	Description
BCLK{0,1,2,3}_DN/DP	Reference Clock Differential input. These pins provide the required reference inputs to various PLLs inside the processor, such as Intel® UPI and PCIe. BCLK0, BCLK1, BCLK2 and BCLK3 run at 100 MHz from the same clock source.
CD_PE_REFCLK_DN/DP	PCIe link Reference Clock for companion die.

3.7 JTAG and TAP Signals

Table 27. JTAG and TAP Signals

Signal Name	Description
BPM_N[7:0]	Breakpoint and Performance Monitor Signals: I/O signals from the processor that indicate the status of breakpoints and programmable counters used for monitoring processor performance. These are 100 MHz signals.
PRDY_N	Probe Mode Ready is a processor output used by debug tools to determine processor debug readiness.
PREQ_N	Probe Mode Request is used by debug tools to request debug operation of the processor.
TCK	Test Clock (TCK) provides the clock input for the processor Test Bus (also known as the Test Access Port).
TDI	Test Data In (TDI) transfers serial test data into the processor. TDI provides the serial input needed for JTAG specification support.
TDO	Test Data Out (TDO) transfers serial test data out of the processor. TDO provides the serial output needed for JTAG specification support.
TMS	Test Mode Select (TMS) is a JTAG specification support signal used by debug tools.

3.8 Serial VID Interface (SVID) Signals

Table 28. SVID Signals

Signal Name	Description
SVIDALERT_N [1:0]	Serial VID alert
SVIDCLK [1:0]	Serial VID clock
SVIDDATA [1:0]	Serial VID data out

3.9 Processor Asynchronous Sideband and Miscellaneous Signals

Table 29. Processor Asynchronous Sideband Signals

Signal Name	Description
CATERR_N	Indicates that the system has experienced a fatal or catastrophic error and cannot continue to operate. The processor will assert CATERR_N for unrecoverable machine check errors and other internal unrecoverable errors. It is expected that every processor in the system will wire-OR CATERR_N for all processors. Since this is an I/O land, external agents are allowed to

continued...

Signal Name	Description
	assert this land which will cause the processor to take a machine check exception. The CATERR_N signal can be sampled any time after 1.5 ms after the assertion of PWRGOOD. On 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids, CATERR_N is used for signaling the following types of errors: • Legacy MCERR's, CATERR_N is asserted for 16 BCLKs.
ERROR_N[2:0]	Error status signals for integrated I/O (IIO) unit: 0 = Hardware correctable error (no operating system or firmware action necessary). 1 = Non-fatal error (operating system or firmware action required to contain and recover). 2 = Fatal error (system reset likely required to recover).
MEM_HOT_C{012/345}_N	Memory throttle control. Signals external BMC-less controller that DIMM is exceeding temperature limit and needs to increase to max fan speed. MEM_HOT_C012_N and MEM_HOT_C345_N signals have two modes of operation - input and output mode. Input mode is externally asserted and is used to detect external events such as VR_HOT# from the memory voltage regulator and causes the processor to throttle the appropriate memory channels. Output mode is asserted by the processor known as level mode. In level mode, the output indicates that a particular branch of memory subsystem is hot. MEM_HOT_C012_N is used for memory channels 0, 1, and 2 while MEM_HOT_C345_N is used for memory channels 3, 4, and 5.
PMSYNC[6:0]	Power Management Sync. A sideband signal to communicate power management status from the Platform Controller Hub (PCH) to the processor.
PROCHOT_N	PROCHOT_N will go active when the processor temperature monitoring sensor detects that the processor has reached its maximum safe operating temperature. This indicates that the processor Thermal Control Circuit has been activated, if enabled. This signal can also be driven to the processor to activate the Thermal Control Circuit. This signal is sampled after PWRGOOD assertion.
PWRGOOD	PWRGOOD is a processor input. The processor requires this signal to be a clean indication that all processor clocks and power supplies are stable and within their specifications. "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 they come within specification. The signal must then transition monotonically to a high state. PWRGOOD can be driven inactive at any time, but clocks and power must again be stable before a subsequent rising edge of PWRGOOD. PWRGOOD transitions from inactive to active when all supplies except VCCIN are stable. The signal must be supplied to the processor; it is used to protect internal circuits against voltage sequencing issues. It should be driven high throughout boundary scan operation.
PLT_AUX_PWRGOOD	This signal is used to indicate a global reset condition (all use models) as well as VNN is energized and within specification (integrated boot capability only). This is a 3.3V CMOS input signal and goes to on-package CPLD.
RESET_N	Global reset signal. Asserting the RESET_N signal resets the processor to a known state and invalidates its internal caches without writing back any of their contents. Note some PLL, Intel® UPI and error states are not affected by reset and only PWRGOOD forces them to a known state.
THERMTRIP_N	Assertion of THERMTRIP_N (Thermal Trip) indicates one of two possible critical over-temperature conditions: One, the processor junction temperature has reached a level beyond which permanent silicon damage may occur and Two, the system memory interface has exceeded a critical temperature limit set by the BIOS. Measurement of the processor junction temperature is accomplished through multiple internal thermal sensors that are monitored by the Digital Thermal Sensor (DTS). Simultaneously, the Power Control Unit (PCU) monitors external memory temperatures via the dedicated SMBus interface to the DIMMs. If any of the DIMMs exceed the BIOS defined limits, the PCU will signal THERMTRIP_N to prevent damage to the DIMMs. Once activated, the processor will stop all execution and shut down all PLLs. To further protect the processor, its core voltage (VCCIN), VCCD, VCCINFAON, VCCINFAON supplies must be removed following the assertion of THERMTRIP_N. Once activated, THERMTRIP_N remains latched until RESET_N is asserted. While the assertion of the RESET_N signal may de-assert THERMTRIP_N, if the processor's junction temperature remains at or above the trip level, THERMTRIP_N will again be asserted after RESET_N is de-asserted. This

continued...

Signal Name	Description
	signal can also be asserted if the system memory interface has exceeded a critical temperature limit set by the BIOS. The THERMTRIP_N signal can be sampled any time after 1.5 ms after the assertion of PWRGOOD.

Table 30. Miscellaneous Signals

Signal Name	Description
BIST_ENABLE	BIST Enable Strap. Input which allows the platform to enable or disable Built-in Self Test (BIST) on the processor. This signal is pulled up on the die. Refer to Table 9 on page 23 for details.
BMCINIT	BMC Initialization Strap. Indicates whether Service Processor Boot Mode should be used. Used in combination with FRMAGENT and SOCKET_ID inputs. 0: Service Processor Boot Mode Disabled. Example boot modes: Local PCH (this processor hosts a legacy PCH with firmware behind it). 1: Service Processor Boot Mode Enabled. In this mode of operation, the processor performs the absolute minimum internal configuration and then waits for the Service Processor to complete its initialization. The socket boots after receiving a "GO" handshake signal via a firmware scratchpad register. This signal is pulled down on the die, refer to Table 9 on page 23 for details.
DMIMODE_OVERRIDE	BMCINIT, DMIMODE_OVERRIDE, FRMAGENT, and LEGACY_SKT, whether local or remote, whether the boot PCH is attached, whether the socket is legacy and whether port0 is DMI or PCIe.
FRMAGENT	Bootable Firmware Agent Strap. This input configuration strap used in combination with SOCKET_ID to determine whether the socket is a legacy socket, bootable firmware agent is present, and DMI links are used in PCIe mode (instead of DMI3 mode). The firmware flash ROM is located behind the local PCH attached to the processor via the DMI3 interface.This signal is pulled down on the die, refer to Table 9 on page 23 for details.
PMFAST_WAKE_N	Power Management Fast Wake. Enables quick package C3 - C6 exits of all sockets. Asserted if any socket detects a break from package C3 - C6 state requiring all sockets to exit the low power state to service a snoop, memory access, or interrupt. Expected to be wired-OR among all processor sockets within the platform.
PROC_ID [2:0]	Processor ID. This output can be used by the platform to determine if the installed processor is a 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids or a future processor. There is no connection to the processor silicon for this signal. The processor package grounds or floats the pin to set 0 or 1, respectively. 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids 00: Sapphire Rapids 01: Reserved 10: Reserved 11: Reserved Sapphire Rapids-W 00: Reserved 01: Reserved 10: Future Processor 11: Sapphire Rapids-W
RSVD	RESERVED. All signals that are RSVD must be left unconnected on the board.
SAFE_MODE_BOOT	Safe Mode Boot Strap. SAFE_MODE_BOOT allows the processor to wake up safely by disabling all clock gating. This allows BIOS to load registers or patches if required. This signal is sampled after PWRGOOD assertion. The signal is pulled down on the die. Refer to Table 9 on page 23 for details.
SKTOCC_N	SKTOCC_N (Socket Occupied) is used to indicate that a processor is present. This is pulled to ground on the processor package; there is no connection to the processor silicon for this signal.

continued...

Signal Name	Description
SOCKET_ID[2:0]	SOCKET_IDStrap. Socket identification configuration straps for establishing the PECI address and Intel® UPI Node ID. This signal is used in combination with FRMAGENT to determine whether the socket is a legacy socket, bootable firmware agent is present, and DMI links are used in PCIe* mode (instead of DMI3 mode). Each processor socket consumes one Node ID, and there are 128 Home Agent tracker entries. This signal is pulled down on the die. Refer to Table 9 on page 23 for details. SOCKET_ID[1:0] is used for 2S platforms and SOCKET_ID[2:0] is implemented on 4S/8S platforms. This is an asynchronous signal to other clocks in the processor.
TEST[8:1]	Must be individually connected to an appropriate power source or ground through a resistor for proper processor operation.
TXT_AGENT	Intel® Trusted Execution Technology (Intel® TXT) Agent Strap. 0 = Default. The socket is not the Intel® TXT Agent. 1 = The socket is the Intel® TXT Agent. The legacy socket (identified by SOCKET_ID[1:0] = 00b) with Intel® TXT Agent should always set the TXT_AGENT to 1b. This signal is pulled down on the die, refer to Table 9 on page 23 for details.
TXT_PLTEN	Intel® Trusted Execution Technology (Intel® TXT) Platform Enable Strap. 0 = The platform is not Intel® TXT enabled. All sockets should be set to zero. Scalable DP (sDP) platforms should choose this setting if the Node Controller does not support Intel® TXT. 1 = Default. The platform is Intel® TXT enabled. All sockets should be set to one. In a non-scalable DP platform this is the default. When this is set, Intel® TXT functionality requires user to explicitly enable Intel® TXT via BIOS setup. This signal is pulled up on the die, refer to Table 9 on page 23 for details.
LEGACY_SKT	BMCINIT, FRMAGENT, LEGACY_SKT together determine the boot mode (SSP, Intel® UPI Link boot modes, DCF boot), whether local or remote, whether the boot PCH is attached, whether the socket is legacy and whether port0 is DMI or PCIe (Gen 1 and 2). With one exception, this input configuration strap indicates to the processor that it is the legacy socket. The legacy processor must be strapped for NODE ID 0, via the SKIT ID pins. There is only one legacy processor in a partition.
CD_INIT_ERROR	On 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids, Intel® have expanded our capabilities to our on-package PIROM capabilities. In addition to having PIROM features, the processor's on-package CPLD will also perform other functions, including soft-straps setup and voltage rail level shifting functions. The on-package CPLD will perform periodic CRC checking to ensure data integrity, and will assert CD_INIT_ERROR if such error is detected. In such cases when errors are being detected, platform are expected to perform a graceful shutdown, and perform a reboot to see if the error persists. the voltage for this pin is 3.3V VTT open drain driver with a pull up of 10 KΩ.

Table 31. PIROM Signals

Signal Name	Description
PIROM_AD[2:0]	Address for PIROM (Processor Information ROM/OEM scratch pad).
PIROM_SM_WP	Write Protect (WP) can be used to write protect the Scratch EEPROM. The Scratch EEPROM is write- protected when this input is pulled high to VCCSTBY33.
PIROM_SCL	The SMBus Clock (SMBCLK) signal is an input clock which is required for operation of PIROM. This clock is driven by the SMBus controller and is asynchronous to other clocks in the processor.
PIROM_SDA	The SMBus Data (SMBDAT) signal is the data signal for the SMBus. This signal provides the single-bit mechanism for transferring data between SMBus devices.

3.10 Processor Power and Ground Supplies

Table 32. Power and Ground Signals

Signal Name	Description
VCCIN	1.83V - 1.6V input to the Integrated Voltage Regulator (IVR). 10 mV VR steps; V=f(VID,RLL, I) VR14 compliant.
VCCIN_SENSE VSS_VCCIN_SENSE	The remote sense signals for VCCIN rail and are used by the voltage regulator to ensure accurate voltage regulation. These signals must be connected to the voltage regulator feedback circuit, which insures the output voltage remains within specification. See the applicable platform design guide for implementation details.
VCCINFAON	1V rail Infrastructur e Always-On (AON) for early on domains; VR14 compliant, 5 mV VR steps.
VCCINFAON_SENSE VSS_VCCINFAON_SENSE	The remote sense signals for VCCINFAON rail and are used by the voltage regulator to ensure accurate voltage regulation. These signals must be connected to the voltage regulator feedback circuit, which insures the output voltage remains within specification. See the applicable platform design guide for implementation details.
VCCFA_EHV	1.8V rail for PCIe 5.0, UPI I/Os and all other FIVRs; VR13 compliant, 10 mV VR steps.
VCCFA_EHV_SENSE VSS_VCCFA_EHV_SENSE	The remote sense signals for VCCFA_EHV rail and are used by the voltage regulator to ensure accurate voltage regulation. These signals must be connected to the voltage regulator feedback circuit, which insures the output voltage remains within specification. See the applicable platform design guide for implementation details.
VCCFA_EHV_FIVRA	Quiet fixed 1.8V voltage rail for the analog I/O FIVR domains and for the core power for On-Pkg HBM; VR13 compliant, 10 mV VR steps.
VCCFA_EHV_FIVRA_SENSE VSS_VCCFA_EHV_FIVRA_SENSE	The remote sense signals for VCCFA_EHV_FIVRA rail and are used by the voltage regulator to ensure accurate voltage regulation. These signals must be connected to the voltage regulator feedback circuit, which insures the output voltage remains within specification. See the applicable platform design guide for implementation details.
VCCD_HV	1.1V rail for all processor DDR5 memory controllers only, not shared with DDR5 DIMMs; VR13 compliant, 5 mV VR steps.
VCCD_HV_SENSE VSS_VCCD_HV_SENSE	The remote sense signals for VCCD_HV_SENSE rail and are used by the voltage regulator to ensure accurate voltage regulation. These signals must be connected to the voltage regulator feedback circuit, which insures the output voltage remains within specification. See the applicable platform design guide for implementation details.
VCCVNN	Fixed 1V rail to the On Pkg devices and platform CPU GPIO terminations.
VPP_HBM	Fixed 2.5V charge pump voltage for On-Pkg HBM. It is mandatory only for HBM enabled SKUs.
VCC_3P3_AUX	Fixed 3.3V rail for the On-Pkg devices. It is mandatory in both S5 and S0 states.
VSS	Processor ground return.

4.0 PIROM

4.1 Processor Information ROM

The Processor Information ROM (PIROM) is a memory device located on the processor and is accessible via the System Management Bus (SMBus) which contains information regarding the processor's features. These features are listed in Table 33 on page 71.

The 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids processor has an integrated Secured Startup Services (S3M) Module. S3M is a subsystem with integrated microcontroller and firmware plus I/O controllers. Together they provides a diverse set of Boot and security services.

S3M Firmware:

- Can access the scratch pad region.
- Will not access the scratch pad region.

The PIROM resides in the lower half of the memory component (addresses 00 to 7Fh), which is permanently write-protected by Intel. The upper half comprises the Scratch EEPROM (addresses 80 to FFh).

Table 33. Processor Information ROM Table

Offset/ Section	# of Bits	Function	Notes	Examples
Header				
00h	8	Data Format Revision.	Two 4-bit hex digits	Start with 00h
01-02h	16	PIROM Size.	Size in bytes (MSB first)	Use a decimal to hex transfer; 128 bytes = 0080h:
03h	8	Processor Data Address.	Byte pointer, 00h if not present	0Dh
04h	8	Processor Core Data Address.	Byte pointer, 00h if not present	19h
05h	8	Processor Uncore Data Address.	Byte pointer, 00h if not present	21h
06h	8	Cache Data Address.	Byte pointer, 00h if not present	2Bh
07h	8	Package Data Address.	Byte pointer, 00h if not present	32h
08h	8	Voltage Data Address.	Byte pointer, 00h if not present	34h
09h	8	Part Number Data Address.	Byte pointer, 00h if not present	3Eh
0Ah	8	Thermal Data Address.	Byte pointer, 00h if not present	4Dh
0Bh	8	Feature Data Address.	Byte pointer, 00h if not present	54h
0Ch	8	PPIN Data Address.	Byte pointer, 00h if not present	5Eh
Processor Data				

continued...

Offset/ Section	# of Bits	Function	Notes	Examples
0D to 12h	48	S-spec/QDF Number.	Six 8-bit ASCII characters	
13h	7/1	Sample/Production.	First seven bits reserved	0b = Sample, 1b = Production 00000001 = production
14h	8	Number of Cores.	Binary Coded Decimal	24h = 24 Cores
15 h	7/1	Hyper-Threading Support.	First seven bits reserved	0b = no Hyper-Threading, 1b = Hyper-Threading 00000001 = Hyper-Threading
17 to 16h	16	System Clock Speed.	Binary Coded Decimal (Mhz)	0100h = 100 MHz[1]
18h	7/1	Segment.	First seven bits reserved	0b = Server, 1b = Workstation, 00000001 = Workstation
Processor Core Data				
1A to 19h	16	CPUID.	4-bit Binary Coded Decimal	
1Bh	8	Extended Model ID.	4-bit Binary Coded Decimal	08h for 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids 0Ch for 5th Gen Intel® Xeon® Processor Scalable Family, Codename Emerald Rapids
1D to 1Ch	16	Maximum P1 Core Frequency.	4-bit Binary Coded Decimal	2500h = 2500 MHz[1]
1F to 1Eh	16	Maximum P0 Core Frequency.	4-bit Binary Coded Decimal	2800h = 2800 MHz[1]
20h	8	Core Count Indicator.	4-bit Binary Coded Decimal	00b = Sapphire Rapids XCC/ Emerald Rapids XCC 01b = Sapphire Rapids MCC/ Emerald Rapids MCC 10b = Sapphire Rapids EE LCC 11b = Sapphire Rapids EE MCC
Processor Uncore Data				
21h	8	Number of Intel® UPI Links.	4-bit Binary Coded Decimal	04h = four Intel UPI links.
23 to 22h	16	Maximum Intel® UPI Link Transfer Rate.	4-bit Binary Coded Decimal	1600h = 16 GT/s
24h	8	Maximum PCIe Link Transfer Rate.	4-bit Binary Coded Decimal	32h = 32 GT/s[1]
26 to 25h	16	Maximum DDR 1DPC Speed.	4-bit Binary Coded Decimal	4800h = 4800 MT/S
28 to 27h	16	Maximum DDR 2DPC Speed.	4-bit Binary Coded Decimal	4400h = 4400 MT/s
29h	8	High Bandwidth Memory Indicator.	4-bit Binary Coded Decimal	0b = non-HBM 1b = HBM
2Ah	8	Reserved.	Reserved for future use	00000000
Cache Data				
2C to 2Bh	16	MLC Cache Size.	KB in 4-bit Binary Coded Decimal	2048h = 2048KB
2F to 2Dh	24	LLC Cache Size.	KB in 4-bit Binary Coded Decimal	115200h = 115200KB
Package Data				

continued...

Offset/ Section	# of Bits	Function	Notes	Examples
32h	8	Package Type.	4-bit Binary Coded Decimal	First four bits reserved Output decode is next.
33h	8	Reserved.	Reserved for future use	0000000000000000
Voltage Data				
35 to 34h	16	Maximum VCCIN.	4-bit Binary Coded Decimal	2000h = 2000 mV[1]
37 to 36h	16	Minimum VCCIN.	4-bit Binary Coded Decimal	1600h = 1600 mV[1]
3D to 38h	48	Reserved.	Reserved for future use	0000000000000000
Part Numbers				
44 to 3Eh	56	Processor Family Number.	Seven 8-bit ASCII characters	CM80645
4C to 45h	64	Processor SKU Number.	Eight 8-bit ASCII characters	41272834
Thermal Reference				
4Dh	8	Tcase Maximum.	4-bit Binary Coded Decimal	69h = 69°C[1]
4F to 4Eh	16	Thermal Design Power.	4-bit Binary Coded Decimal	350h = 350W [1]
51 to 50h	16	DTS Maximum.	4-bit Binary Coded Decimal	95h = 95°C[1]
53 to 52h	16	Pn Limit.	4-bit Binary Coded Decimal	53h = 53W[1]
Features				
57 to 54h	32	Processor Core Feature Flags.	From CPUID function 1, EDX contents	4387FBFFh
59 to 58h	16	Processor Feature Flags.	Up to 16 features - Binary 1 indicates functional feature	0000000000001111
5Ah	5/3	Multiprocessor Support.	0=1S, 1=2S, 2=4S, 3=S4S, 4=S8S	00000011 = S4S
5Bh	8	Number of Devices in TAP Chain.	4-bit Binary Coded Decimal	11h = 10 cores
5Ch	8	Static Checksum.	1-byte checksum	Add up by byte and take 2's complement.
5Dh	8	Reserved.	Reserved for future use	0000000000000000
Other				
65 to 5Eh	64	PPIN	Coded binary	See description.
7Fh to 66h	208	Reserved.	Reserved for future use	

Notes:
1. Uses Binary Coded Decimal (BCD) translation.

4.2 Scratch EEPROM

Also available in the memory component on the processor SMBus is an EEPROM which may be used for other data at the system or processor vendor’s discretion. The data in this EEPROM, once programmed, can be write-protected by asserting the active-high SM_WP signal. This signal has a weak pull-down (10 KΩ) to allow the EEPROM to be programmed in systems with no implementation of this signal. The Scratch EEPROM

resides in the upper half of the memory component (addresses 80 - FFh). The lower half comprises the Processor Information ROM (addresses 00 - 7Fh), which is permanently write-protected by Intel.

4.3 PIROM and Scratch EEPROM Supported SMBus Transactions

The PIROM responds to two SMBus packet types: Read Byte and Write Byte. However, since the PIROM is write-protected, it will acknowledge a Write Byte command but ignore the data. The Scratch EEPROM responds to Read Byte and Write Byte commands. Table 34 on page 74 illustrates the Read Byte command. Table 35 on page 74 illustrates the Write Byte command.

In the tables, 'S' represents a SMBus start bit, 'P' represents a stop bit, 'A' represents an acknowledge (ACK), and '///' represents a negative acknowledge (NACK). The shaded bits are transmitted by the PIROM or Scratch EEPROM, and the bits that are not shaded are transmitted by the SMBus host controller. In the tables, the data addresses indicate eight bits.

The SMBus host controller should transmit eight bits with the most significant bit indicating which section of the EEPROM is to be addressed: the PIROM (MSB = 0) or the Scratch EEPROM (MSB = 1).

Table 34. Read Byte SMBus Packet

S	Slave Address	Write	A	Command Code	A	S	Slave Address	Read	A	Data	///	P
1	7-bits	1	1	8-bits	1	1	7-bits	1	1	8-bits	1	1

Table 35. Write Byte SMBus Packet

S	Slave Address	Write	A	Command Code	A	Data	A	P
1	7-bits	1	1	8-bits	1	8-bits	1	1

4.4 SMBus Memory Component Addressing

Of the addresses broadcast across the SMBus, the memory component claims those of the form "10100XXZb". The "XX" bits are defined by pull-up and pull-down of the PIROM_ADDR[2:0] pins. These address pins are pulled down weakly (10k) on the processor substrate to ensure that the memory components are in a known state in systems which do not support the SMBus (or only support a partial implementation). The "Z" bit is the read/write bit for the serial bus transaction.

Note that addresses of the form "0000XXXXb" are Reserved and should not be generated by an SMBus master.

Table 36 on page 75 describes the address pin connections and how they affect the addressing of the memory component.

Table 36. Memory Device SMBus Addressing

Address (Hex)	Upper Address[1]	Device Select			R/W
	Bits 7-4	PIROM_ADDR[2]	PIROM_ADDR[1]	PIROM_ADDR[0]	Bit 0
A0h/A1h	1010	0	0	0	X
A2h/A3h	1010	0	0	1	X
A4h/A5h	1010	0	1	0	X
A6h/A7h	1010	0	1	1	X
A8h/A9h	1010	1	0	0	X
AAh/ABh	1010	1	0	1	X
ACh/ADh	1010	1	1	0	X
AEh/AFh	1010	1	1	1	X

1. This addressing scheme will support up to four processors on a single SMBus.

4.4.1 Managing Data in the PIROM

The PIROM consists of the following sections:

- Header
- Processor Data
- Processor Core Data
- Processor Uncore Data
- Cache Data
- Package Data
- Part Number Data
- Thermal Reference Data
- Feature Data
- Other Data

Details on each of these sections are described next.

NOTE

Reserved fields or bits SHOULD be programmed to zeros. However, OEMs should not rely on this model.

4.4.2 Header

To maintain backward compatibility, the Header defines the starting address for each subsequent section of the PIROM. Software should check for the offset before reading data from a particular section of the ROM.

Example: Code looking for the processor uncore data of a processor would read offset 05h to find a value of 21. 21 is the first address within the 'Processor Uncore Data' section of the PIROM.

4.4.2.1 DFR: Data Format Revision

This location identifies the data format revision of the PIROM data structure. Writes to this register have no effect.

Offset: 00h	
Bit	**Description**
7:0	**Data Format Revision** The data format revision is used whenever fields within the PIROM are redefined. The initial definition will begin at a value of 1. If a field, or bit assignment within a field, is changed such that software needs to discern between the old and new definition, then the data format revision field will be incremented. 00h: Reserved 01h: Initial definition 02h: Second revision 03h: Third revision 04h: Fourth revision 05h: Fifth revision 06h:Sixth revision 07h:Seventh revision 08h:Eighth revision 09h:Ninth revision (Defined by this document) 0A-FFh: Reserved

4.4.2.2 PISIZE: PIROM Size

This location identifies the PIROM size. Writes to this register have no effect.

Offset: 01h-02h	
Bit	**Description**
15:0	**PIROM Size** The PIROM size provides the size of the device in hex bytes. The MSB is at location 01h; the LSB is at location 02h. 0000h - 007Fh: Reserved 0080h: 128 byte PIROM size 0081- FFFFh: Reserved

4.4.2.3 PDA: Processor Data Address

This location provides the offset to the Processor Data Section. Writes to this register have no effect.

Offset: 03h	
Bit	**Description**
7:0	**Processor Data Address** Byte pointer to the Processor Data section 0Dh: Processor Data section pointer value

4.4.2.4 PCDA: Processor Core Data Address

This location provides the offset to the Processor Core Data Section. Writes to this register have no effect.

Offset: 04h	
Bit	**Description**
7:0	**Processor Core Data Address** Byte pointer to the Processor Core Data section 19h: Processor Core Data section pointer value

4.4.2.5 PUDA: Processor Uncore Data Address

This location provides the offset to the Processor Uncore Data Section. Writes to this register have no effect.

Offset: 05h	
Bit	**Description**
7:0	**Processor Uncore Data Address** Byte pointer to the Processor Uncore Data section 21h: Processor Uncore Data section pointer value

4.4.2.6 CDA: Cache Data Address

This location provides the offset to the Cache Data Section. Writes to this register have no effect.

Offset: 06h	
Bit	**Description**
7:0	**Cache Data Address** Byte pointer to the Cache Data section 2Bh: Cache Data section pointer value

4.4.2.7 PNDA: Package Data Address

This location provides the offset to the Package Data Section. Writes to this register have no effect.

Offset: 07h	
Bit	**Description**
7:0	**Package Data Address** Byte pointer to the Package Data section 32h: Package Data section pointer value

4.4.2.8 VDA: Voltage Data Address

This location provides the offset to the Voltage Data Section. Writes to this register have no effect.

Offset: 08h	
Bit	**Description**
7:0	**Voltage Data Address** Byte pointer to the Voltage Data section 34h: Voltage Data section pointer value

4.4.2.9 PNDA: Part Number Data Address

This location provides the offset to the Part Number Data Section. Writes to this register have no effect.

Offset: 09h	
Bit	**Description**
7:0	**Part Number Data Address** Byte pointer to the Part Number Data section 3Eh: Part Number Data section pointer value

4.4.2.10 TRDA: Thermal Reference Data Address

This location provides the offset to the Thermal Reference Data Section. Writes to this register have no effect.

Offset: 0Ah	
Bit	**Description**
7:0	**Thermal Reference Data Address** Byte pointer to the Thermal Reference Data section 4Dh: Thermal Reference Data section pointer value

4.4.2.11 FDA: Feature Data Address

This location provides the offset to the Feature Data Section. Writes to this register have no effect.

Offset: 0Bh	
Bit	**Description**
7:0	**Feature Data Address** Byte pointer to the Feature Data section 54h: Feature Data section pointer value

4.4.2.12 PPIN: Protected Processor Inventory Number

This location provides the offset to the PPIN Data Section. Writes to this register have no effect.

Offset: 0Ch	
Bit	**Description**
7:0	**PPIN Data Address** Byte pointer to the PPIN Data section 5Eh: PPIN Data section pointer value

4.4.3 Processor Data

This section contains five pieces of data:

- The S-spec/QDF of the part in ASCII format.
- (1) 2-bit field to declare if the part is a pre-production sample or a production unit.

- Core count.
- Intel® Hyper-threading Technology support status.
- The system bus speed in BCD format.

4.4.3.1 SQNUM: S-Spec QDF Number

This location provides the S-Spec or QDF number of the processor. The S-spec/QDF field is six ASCII characters wide and is programmed with the same S-spec/QDF value as marked on the processor. If the value is less than six characters in length, leading spaces (20h) are programmed in this field. Writes to this register have no effect.

For example, a processor with a QDF mark of QWFZ contains the following in field 0D-12h: 20h, 20h, 51h, 57h, 46h, 5Ah. This data consists of two blanks at 0Dh and 0Eh followed by the ASCII codes for QEU5 in locations 0F - 12h.

Offset: 0Dh-12h	
Bit	**Description**
7:0	**Character 6** S-Spec or QDF character or 20h 00h-0FFh: ASCII character
15:8	**Character 5** S-Spec or QDF character or 20h 00h-0FFh: ASCII character
23:16	**Character 4** S-Spec or QDF character 00h-0FFh: ASCII character
31:24	**Character 3** S-Spec or QDF character 00h-0FFh: ASCII character
39:32	**Character 2** S-Spec or QDF character 00h-0FFh: ASCII character
47:40	**Character 1** S-Spec or QDF character 00h-0FFh: ASCII character

4.4.3.2 SAMPROD: Sample/Production

This location contains the sample/production field, which is a two-bit field and is LSB aligned. All Q-spec material will use a value of 00b. All S-spec material will use a value of 01b. All other values are reserved. Writes to this register have no effect.

For example, a processor with a Qxxx mark (engineering sample) will have offset 13h set to 00h. A processor with an Sxxxx mark (production unit) will use 01h at offset 13h.

Offset: 13h	
Bit	**Description**
7:2	**RESERVED**

continued...

Offset: 13h	
Bit	**Description**
	000000b-111111b: Reserved
1:0	**Sample/Production** Sample or Production indicator 00b: Sample 01b: Production 10b-11b: Reserved

4.4.3.3 Processor Core Information

This location contains information regarding the number of cores on the processor. Writes to this register have no effect. Data format is binary coded decimal.

For example, the 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids server processor has up to 56 cores.

Offset: 14h	
Bit	**Description**
7:0	**Number of cores** 0000h-FFFFh: Cores

4.4.3.4 Hyper-Threading Support

This location contains information whether Hyper-Threading is supported or not.

0b = no Hyper-Threading

1b = Hyper-Threading

Offset: 15h	
Bit	**Description**
7:0	**Hyper-Threading** 0000h-FFFFh: Hyper-Threading

4.4.3.5 SCS: System Clock Speed

This location contains the system clock frequency information. Systems may need to read this offset to decide if all installed processors support the same system clock speed. The data provided is the speed, rounded to a whole number, and reflected in binary coded decimal. Writes to this register have no effect.

For example, a processor with system bus speed of 100 MHz will have a value of 0100h.

Offset: 17h-16h	
Bit	**Description**
15:0	**System Clock Speed** 0000h-FFFFh: MHz

4.4.3.6 Segment

This location contains information of the segment.

0b = Server

1b = Workstation

Offset: 18h	
Bit	**Description**
7:0	**Segment** 0000h-FFFFh

4.4.4 Processor Core Data

This section contains silicon-related data relevant to the processor cores.

4.4.4.1 CPUID: CPUID

This location contains the CPUID, Processor Type, Family, Model and Stepping. The CPUID field is a copy of the results in EAX[15:0] from Function 1 of the CPUID instruction. Writes to this register have no effect. Data format is hexadecimal.

Offset: 1Ah-19h	
Bit	**Description**
15:13	**Reserved** 00b-11b: Reserved
12:12	**Processor Type** 0b-1b: Processor Type
11:8	**Processor Family** 0h-Fh: Processor Family
7:4	**Processor Model** 0h-Fh: Processor Model
3:0	**Processor Stepping** 0h-Fh: Processor Stepping

4.4.4.2 Extended Model ID

This location contains Extended Model ID. Writes to this register have no effect.

Offset: 1Bh	
Bit	**Description**
7:0	**Extended Model ID** 0h-Fh: Extended Model ID

4.4.4.3 MP1CF: Maximum P1 Core Frequency

This location contains the maximum non Intel® Turbo Boost Technology core frequency for the processor. The frequency should equate to the markings on the processor and/or the QDF/S-spec speed even if the parts are not limited or locked to the intended speed. Format of this field is in megahertz, rounded to a whole number, and encoded in binary coded decimal. Writes to this register have no effect.

Example: A 2.6 GHz processor will have a value of 2600h.

Offset: 1D-1CH	
Bit	**Description**
15:0	**Maximum P1 Core Frequency** 0000h-FFFFh: MHz

4.4.4.4 MP0CF: Maximum P0 Core Frequency

This location contains the maximum Intel® Turbo Boost Technology core frequency for the processor. This is the maximum intended speed for the part under any functional conditions. Format of this field is in megahertz, rounded to a whole number, and encoded in binary coded decimal. Writes to this register have no effect.

Example: A processor with a maximum Intel® Turbo Boost Technology frequency of 2.8 GHz will have a value of 2800h.

Offset: 1Fh-1Eh	
Bit	**Description**
15:0	**Maximum P0 Core Frequency** 0000h-FFFFh: MHz

4.4.4.5 Core Count Indicator

This location differentiates Sapphire Rapids XCC/Emerald Rapids XCC, Sapphire Rapids MCC/Emerald Rapids MCC, Sapphire Rapids EE LCC, and Sapphire Rapids EE MCC. Writes to this register have no effect. Data format is binary coded decimal.

Offset: 20h	
Bit	**Description**
7:0	**Core Count Indicator: CPU SKU** 00b = Sapphire Rapids XCC/Emerald Rapids XCC 01b = Sapphire Rapids MCC/Emerald Rapids MCC 10b = Sapphire Rapids EE LCC 11b = Sapphire Rapids EE MCC

4.4.5 Processor Uncore Data

This section contains silicon-related data relevant to the processor Uncore.

4.4.5.1 UPIL: Number of Intel UPI Links

Systems may need to read this offset to decide if the device has enough Intel® UPI Links to operate the number of processors your system is capable of supporting. The data provided is the number of links, and reflected in binary coded decimal. Writes to this register have no effect.

Example: The 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids supports a maximum of four links. Therefore, offset 21h could have a value of 04.

Offset: 21h	
Bit	**Description**
7:0	**Number of Intel® UPI links** 00h-FFh: Links

4.4.5.2 MAXUPI: Maximum Intel UPI Transfer Rate

Systems may need to read this offset to decide if all installed processors support the same Intel® UPI link transfer rate. The data provided is the transfer rate, rounded to a whole number, and reflected in binary coded decimal. Writes to this register have no effect.

Example: When the 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids supports a maximum Intel® UPI link transfer rate of 16 GT/s then this offset 22h-23h has a value of 1600.

Offset: 23h-22h	
Bit	**Description**
15:0	**Maximum Intel® UPI Transfer Rate** 0000h-FFFFh: 10 MHz

4.4.5.3 MAXPCI: Maximum PCIe Transfer Rate

Systems may need to read this offset to decide if all installed processors support the same PCIe Link Transfer Rate. The data provided is the transfer rate, rounded to a whole number, and reflected in binary coded decimal. Writes to this register have no effect.

For example, the 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids supports a maximum PCIe transfer rate of 32 GT/s.

Offset: 24h	
Bit	**Description**
7:0	**Maximum PCIe Transfer Rate** 00h-FFh: MHz

4.4.5.4 DDR1DPC: Maximum Intel DDR5 1 DPC DIMM Speed

Systems may need to read this offset to set maximum DIMM speeds supporting the 1 DPC usage. The data provided is maximum supported DIMM frequency, rounded to a whole number, and reflected in binary coded decimal. Writes to this register have no effect.

Example: The Eagle Stream platform supports a maximum 1DPC DDR5 frequency of 4800 MT/s for 4th Gen Intel® Xeon® Scalable Processors and 5600 MT/s for 5th Gen Intel® Xeon® Scalable Processors.

Offset: 26h-25h	
Bit	**Description**
15:0	**Maximum Intel DDR5 1DPC Speed** 0000h-FFFFh: MHz

4.4.5.5 DDR2DPC: Maximum Intel DDR5 2 DPC DIMM Speed

Systems may need to read this offset to set maximum DIMM speeds supporting the 2DPC usage. The data provided is maximum supported DIMM frequency, rounded to a whole number, and reflected in binary coded decimal. Writes to this register have no effect.

Example: The Eagle Stream platform supports a maximum 2DPC DDR5 frequency of 4400 MT/s for 4th Gen Intel® Xeon® Scalable Processors and 4800 MT/s for 5th Gen Intel® Xeon® Scalable Processors.

Offset: 28h-27h	
Bit	**Description**
15:0	**Maximum Intel's DDR5 2DPC Speed** 0000h-FFFFh: MHz

Note: PIROM reports incorrect 2DPC speed for any 4th Gen Intel® Xeon® Scalable Processor SKUs with less than 4800 MT/s 1DPC speed. Following is the list of SKUs reporting wrong 2DPC speed for 4th Gen Intel® Xeon® Scalable Processors. Software should ignore the 2DPC speed read out of PIROM for any of the affected SKUs (shown in the previous table). Alternately, software can assume that the 2DPC speed for any SKU with 1DPC speed less than 4800 MT/s is EQUAL to the 1DPC speed.

Processor Number	CPU BRAND STRING	1DPC	2DPC
6430	Intel® Xeon® Gold 6430	4400	4400
C6430	Montage Jintide* C6430	4400	4400
3408U	Intel® Xeon® Bronze 3408U	4000	4000
5415+	Intel® Xeon® Gold 5415+	4400	4400
4410Y	Intel® Xeon® Silver 4410Y	4000	4000
4416+	Intel® Xeon® Silver 4416+	4000	4000
5418Y	Intel® Xeon® Gold 5418Y	4400	4400
5412U	Intel® Xeon® Gold 5412U	4400	4400
5420+	Intel® Xeon® Gold 5420+	4400	4400
4410T	Intel® Xeon® Silver 4410T	4000	4000

continued...

Processor Number	CPU BRAND STRING	1DPC	2DPC
5418N	Intel® Xeon® Gold 5418N	4000	4000
5411N	Intel® Xeon® Gold 5411N	4400	4400
6428N	Intel® Xeon® Gold 6428N	4000	4000
6421N	Intel® Xeon® Gold 6421N	4400	4400
5416S	Intel® Xeon® Gold 5416S	4400	4400
C4410Y	Montage Jintide* C4410Y	4000	4000
C4416+	Montage Jintide* C4416+	4000	4000
C5418Y	Montage Jintide* C5418Y	4400	4400
C5420+	Montage Jintide* C5420+	4400	4400
C5416S	Montage Jintide* C5416S	4400	4400
C5415+	Montage Jintide* C5415+	4400	4400

4.4.5.6 High Bandwidth Memory Indicator

This location contains information to differentiate HBM SKUs from non-HBM.

0b = non-HBM

1b = HBM

Offset: 29h	
Bit	**Description**
7:0	High Bandwidth Memory Indicator 00h-FFh

4.4.5.7 RES1: Reserved 1

This locations are reserved. Writes to this register have no effect.

Offset: 2Ah	
Bit	**Description**
8:0	**RESERVED** 00h-FFh: Reserved

4.4.6 Processor Cache Data

This section contains silicon-related data relevant to the processor caches.

4.4.6.1 MLC: Mid Level Cache Size

This location contains the size of the level-two cache in kilobytes per core. Writes to this register have no effect. Data format is decimal.

Example: The 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids has a 2 MB MLC cache per core. Thus, offset 2Bh-2Ch will contain a value of 2048.

Offset: 2Ch-2Bh	
Bit	**Description**
15:0	**Mid Level Cache Size** 0000h-FFFFh: KB

4.4.6.2 LLC: Last Level Cache Size

This location contains the size of the level-three cache in megabytes per package. Writes to this register have no effect. Data format is decimal.

Example: When the 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids has up to a 112.5 MB LLC cache then this offset 2Dh-2Fh will contain a value of 115200.

Offset: 2Fh-2Dh	
Bit	**Description**
23:0	**Last Level Cache Size** 0000h-FFFFh: KB

4.4.6.3 DIMM Max Capacity

This location contains DIMM Max Capacity information. Bit 15:0 is a binary value representation of a multiplier of 64 GB to indicate DIMM Max Capacity. Writes to this register have no effect.

Example: A value of 0 does mean that the DIMM Max Capacity is unlimited.

Offset: 31h-30h	
Bit	**Description**
15:0	**DIMM Max Capacity** 0000h-FFFFh:

4.4.7 Package Data

This section contains substrate and other package related data.

4.4.7.1 PKGT: Package Type

This location tracks the package type. 0 = 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids, 1 = Future generations. Writes to this register have no effect.

Offset: 32h	
Bit	**Description**
7:0	**Package Type** 00h-FFh:

4.4.7.2 RES2: Reserved 2

This location is reserved. Writes to this register have no effect.

Offset: 33h	
Bit	**Description**
7:0	**RESERVED** 00h-FFh: Reserved

4.4.8 Processor Voltage Data

This section contains silicon-related data relevant to the processor voltage rails.

4.4.8.1 MXVCCIN: MAX VCCIN VID

Offset 35h-34h is the Processor VCCIN maximum VID (Voltage Identification) field and contains the maximum voltage requested via the VID pins. This field, rounded to the next thousandth, is in mV and is reflected in binary coded decimal. Some systems read this offset to determine if all processors support the same default VID setting. Writes to this register have no effect.

Example: A voltage of 1.800 mV maximum core VID would contain 1800h in Offset 35h- 34h.

Offset: 35h-34h	
Bit	**Description**
15:0	**MAX VCCIN VID** 0000h-FFFFh: mV

4.4.8.2 MNVCCIN: MIN VCCIN VID

Offset 37h-36h is the Processor Vsa minimum Voltage Identification (VID) field and contains the minimum voltage requested via the VID pins. This field, rounded to the next thousandth, is in mV and is reflected in binary coded decimal. Some systems read this offset to determine if all processors support the same default VID setting. Writes to this register have no effect.

Example: A voltage of 600 mV maximum core VID would contain 600h in Offset 37-36h.

Offset: 37-36h	
Bit	**Description**
15:0	**MIN VCCIN VID** 0000h-FFFFh: mV

4.4.8.3 RES3: Reserved 3

This location is reserved. Writes to this register have no effect.

Offset: 3Dh-38h	
Bit	**Description**
47:0	**RESERVED** 0000h-FFFFh: Reserved

4.4.9 Part Number Data

This section provides device traceability.

4.4.9.1 PFN: Processor Family Number

This location contains seven ASCII characters reflecting the Intel® family number for the processor. This number is the same on all Intel® Xeon® E7 v3 processors. Combined with the Processor SKU Number shown next, this is the complete processor part number. This information is typically marked on the outside of the processor. If the part number is less than 15 total characters, a leading space is inserted into the value. The part number should match the information found in the marking specification. Writes to this register have no effect.

For example, a processor with a part number of AT80604******** will have the following data found at offset 44-3Eh: 41h, 54h, 38h, 30h, 36h, 30h, 34h.

Offset: 44h-3Eh	
Bit	**Description**
7:0	**Character 1** ASCII character 00h-0FFh: ASCII character
15:8	**Character 2** ASCII character 00h-0FFh: ASCII character
23:16	**Character 3** ASCII character 00h-0FFh: ASCII character
31:24	**Character 4** ASCII character 00h-0FFh: ASCII character
39:32	**Character 5** ASCII character 00h-0FFh: ASCII character
47:40	**Character 6** ASCII character 00h-0FFh: ASCII character
55:48	**Character 7** ASCII character 00h-0FFh: ASCII character

4.4.9.2 PSN: Processor SKU Number

This location contains eight ASCII characters reflecting the SKU number for the processor. Added to the end of the Processor Family Number shown previously, this is the complete processor part number. This information is typically marked on the outside of the processor. If the part number is less than 15 total characters, a leading space is inserted into the value. The part number should match the information found in the marking specification. Writes to this register have no effect.

Example: A processor with a part number of *******003771AA will have the following data found at offset 4C-45h: 30h, 30h, 33h, 37h, 37h, 31h, 41h, 41h.

Offset: 4Ch-45h	
Bit	**Description**
7:0	**Character 1** ASCII character 00h-0FFh: ASCII character
15:8	**Character 2** ASCII character 00h-0FFh: ASCII character
23:16	**Character 3** ASCII character 00h-0FFh: ASCII character
31:24	**Character 4** ASCII character 00h-0FFh: ASCII character
39:32	**Character 5** ASCII character 00h-0FFh: ASCII character
47:40	**Character 6** ASCII character 00h-0FFh: ASCII character
55:48	**Character 7** ASCII character 00h-0FFh: ASCII character
63:56	**Character 8** ASCII character 00h-0FFh: ASCII character

4.4.10 Thermal Reference Data

4.4.10.1 TCASE: TCASE Maximum

This location provides the maximum T_{CASE} for the processor. The field reflects temperature in degrees Celsius in binary coded decimal format. The thermal specifications are specified at the case Integrated Heat Spreader (IHS). Writes to this register have no effect.

Example: A temperature of 66°C would contain a value of 66h.

Offset: 4Dh	
Bit	**Description**
7:0	**T_{CASE} Maximum** 00h-FFh: Degrees Celsius

4.4.10.2 TDP: Thermal Design Power

This location contains the maximum Thermal Design Power for the part. The field reflects power in watts in binary coded decimal format. Writes to this register have no effect. A zero value means that the value was not programmed.

Example: A 350 W TDP would be saved as 0350h.

Offset: 4Fh-4Eh	
Bit	**Description**
15:0	**Thermal Design Power** 0000h-FFFFh: Watts

4.4.10.3 DTSMAX: Digital Thermal Sensor Maximum

This location provides the Digital Thermal Sensor Maximum temperature for the processor. The field reflects temperature in degrees Celsius in binary coded decimal format. The thermal specifications are specified at the sensor nearest the CPU hot spot. Writes to this register have no effect.

Example: A temperature of 103°C would contain a value of 0103h.

Offset: 51h-50h	
Bit	**Description**
15:0	**Digital Thermal Sensor Maximum** 0000h-FFFFh: Degrees Celsius

4.4.10.4 PN: Pn Power Limit

This location contains the maximum Pn power for the part. The field reflects power in watts in binary coded decimal format. Writes to this register have no effect. A zero value means that the value was not programmed.

Example: A 35 W would be saved as 0035h.

Offset: 53h-52h	
Bit	**Description**
15:0	**Pn Power Limit** 0000h-FFFFh: Watts

4.4.11 Feature Data

This section provides information on key features that the platform may need to understand without powering on the processor.

4.4.11.1 PCFF: Processor Core Feature Flags

This location contains a copy of results in EDX[31:0] from Function 1 of the CPUID instruction. These details provide instruction and feature support by product family. Writes to this register have no effect.

Example: A value of BFEBFBFFh can be found at offset 57h - 54h.

Offset: 57h-54h	
Bit	**Description**
31:0	**Processor Core Feature Flags** 00000000h-FFFFFFFFF: Feature Flags

4.4.11.2 PFF: Processor Feature Flags

This location contains additional feature information from the processor. Writes to this register have no effect.

Offset: 59h-58h		
Bit	**Bit**	**Description**
	71h	Reserved
		Reserved
		Reserved
		Reserved
		Reserved
		Reserved
		Reserved
		Reserved
7	70h	Reserved
6		Reserved
5		Intel® Speed Select Technology (Intel® SST) Enabled
4		AEP Enabled
3		Intel® TXT Enabled
2		EMCA2 Enabled
1		Turbo Enabled
0		avx512_2ndFMA

Bits are set when a feature is present, and cleared when they are not.

4.4.11.3 MPSUP: Multiprocessor Support

This location contains three bits for representing the supported number of physical processors on the bus. These two bits are LSB aligned where 000b equates to non-scalable 1 socket (1S) operation, 001b to 2 socket (2S), 010b to non-scalable 4 socket (4S), 011 to scalable 4 socket (S4S), and 100 scalable 8 socket (S8S). The 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids is a 1S, 2S, 4S, or 8S processor. The first six bits in this field are reserved for future use. Writes to this register have no effect.

Example: A scalable 8-socket processor will have a value of 100h at offset 5Ah.

Offset: 5Ah	
Bit	**Description**
7:3	**RESERVED** 000000b-111111b: Reserved
2:0	**Multiprocessor Support** 1S, 2S, 4S, S4S or S8S indicator 000b: Non-scalable 1 Socket 001b: 2 Socket
	continued...

Offset: 5Ah	
Bit	**Description**
	010b: Non-scalable 4 Socket 011b: Scalable 4 Socket 100b: Scalable 8 Socket

4.4.11.4 TCDC: Tap Chain Device Count

At offset 5B, a 4-bit binary coded decimal is used to tell how many devices are in the TAP Chain. In a 4th Gen Intel® Xeon® Processor Scalable Family, Codename Sapphire Rapids with ten cores, this field would be set to 11h.

Offset: 5Bh	
Bit	**Description**
7:0	**TAP Chain Device Count** 0000h-FFFFh

4.4.11.5 STTCKS: Static Checksum

This location provides the checksum of the static values per SKU. Writes to this register have no effect.

Offset: 5Ch	
Bit	**Description**
7:0	**Static Checksum** One-byte checksum of the Static Checksum 00h- FFh: See Checksums on page 93 for calculation of this value.

4.4.11.6 RES4: Reserved 4

This location is reserved. Writes to this register have no effect

Offset: 5Dh	
Bit	Description
7:00	**RESERVED** 00h-FFh: Reserved

4.4.12 Protected Processor Inventory Number

This section contains the Protected Processor Inventory Number and checksum.

4.4.12.1 PPIN: Protected Processor Inventory Number

This location contains a 64-bit identification number. The value in this field is the PPIN number, which will be the same value as the PPIN accessed through the BIOS MSR. Writes to this register have no effect.

Offset: 65h-5Eh	
Bit	**Description**
63:0	**PPIN**

Offset: 65h-5Eh	
Bit	**Description**
	0000000000000000h-FFFFFFFFFFFFFFFFh: PPIN

4.4.12.2 RES5: Reserved 5

This location is reserved. Writes to this register have no effect.

Offset: 7Fh-66h	
Bit	**Description**
207:0	**RESERVED** 00h- FFh: Reserved.

4.4.13 Checksums

The PIROM includes multiple checksums. Table 37 on page 93 includes the checksum values for each section defined in the 128-byte ROM.

Table 37. Byte ROM Checksum Values

Section	Checksum Address
Static Features	5Ch

Checksums are automatically calculated and programmed by Intel. The first step in calculating the checksum is to add each byte from the field to the next subsequent byte. This result is then negated to provide the checksum.

Example: For a byte string of AA445Ch, the resulting checksum will be B6h.

- — AA = 10101010 44 = 01000100 5C = 01011100
  — AA + 44 + 5C = 01001010

Negate the sum: 10110101 +1 = **10110110 (B6h)**