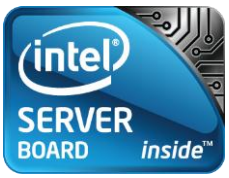
Intel® Server Board S2600IP and Intel® Workstation Board W2600CR

Technical Product Specification

Intel order number G34153-002



Revision 1.0

February, 2012

Enterprise Platforms and Services Division - Marketing

Revision History

Date	Revision Number	Modifications
February 2012	1.0	Initial release.

Disclaimers

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, lifesaving, or life sustaining applications. Intel may make changes to specifications and product descriptions at any time, without notice.

Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

The Intel® Server Board S2600IP and Intel® Workstation Board W2600CR 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 and the software described in it is furnished under license and may only be used or copied in accordance with the terms of the license. The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document.

Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

Intel, Pentium, Itanium, and Xeon are trademarks or registered trademarks of Intel Corporation.

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

Table of Contents

List of Figures

List of Tables

<This page is intentionally left blank.>

1. Introduction

This Technical Product Specification (TPS) provides board-specific information detailing the features, functionality, and high-level architecture of the Intel® Server Board S2600IP and Intel® Workstation Board W2600CR.

In addition, you can obtain design-level information for a given subsystem by ordering the External Product Specifications (EPS) for the specific subsystem. EPS documents are not publicly available and you must order them through your local Intel representative.

1.1 Chapter Outline

This document is divided into the following chapters:

- Chapter 1 – Introduction
- Chapter 2 – Product Overview
- Chapter 3 – Functional Architecture
- Chapter 4 – Platform Management Overview
- Chapter 5 – System Security
- Chapter 6 – Connector/Header Locations and Pin-outs
- Chapter 7 – Jumper Blocks
- Chapter 8 – Intel® Light Guided Diagnostics
- Chapter 9 – Design and Environmental Specifications
- Appendix A: Integration and Usage Tips
- Appendix B: Compatible Intel® Server Chassis
- Appendix C: BMC Sensor Tables
- Appendix D: POST Code Diagnostic LED Decoder
- Appendix E: POST Error Messages and Handling
- Glossary
- Reference Documents

1.2 Server Board Use Disclaimer

Intel® Server Boards contain a number of high-density VLSI (Very-large-scale integration) and power delivery components that require adequate airflow for cooling. Intel ensures through its own chassis development and testing that when Intel® server building blocks are used together, the fully integrated system meets the intended thermal requirements of these components. It is the responsibility of the system integrator who chooses not to use Intel developed server building blocks to consult vendor datasheets and operating parameters to determine the amount of airflow required for their specific application and environmental conditions. Intel Corporation cannot be held responsible if components fail or the server board does not operate correctly when used outside any of the published operating or non-operating limits.

2. Product Overview

The Intel® Server Board S2600IP and Intel® Workstation Board W2600CR are Enterprise I/O Rich platforms for Pedestal and Rack Server and workstation market.

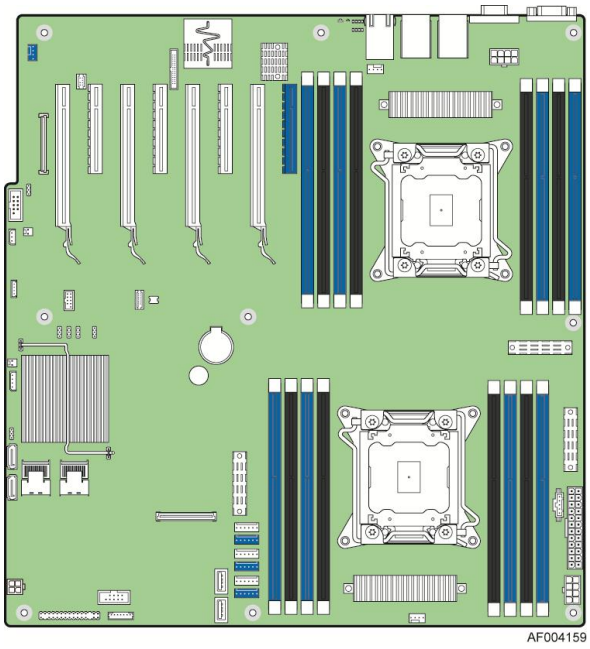


Figure 1. Intel® Server Board S2600IP

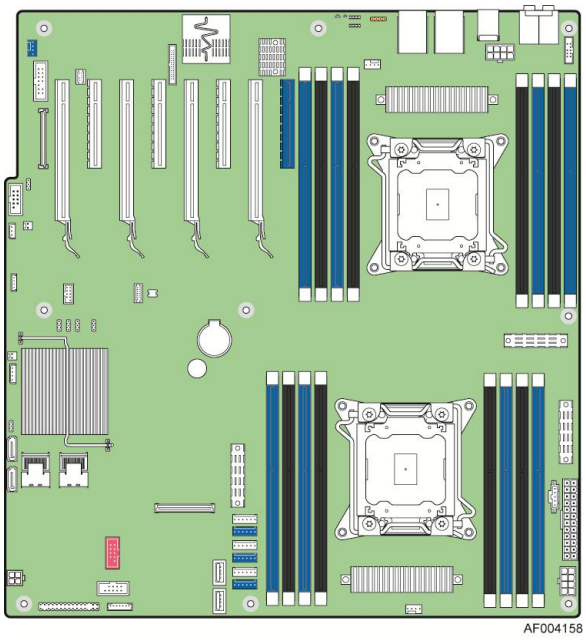


Figure 2. Intel® Workstation Board W2600CR

2.1 Product Feature Set

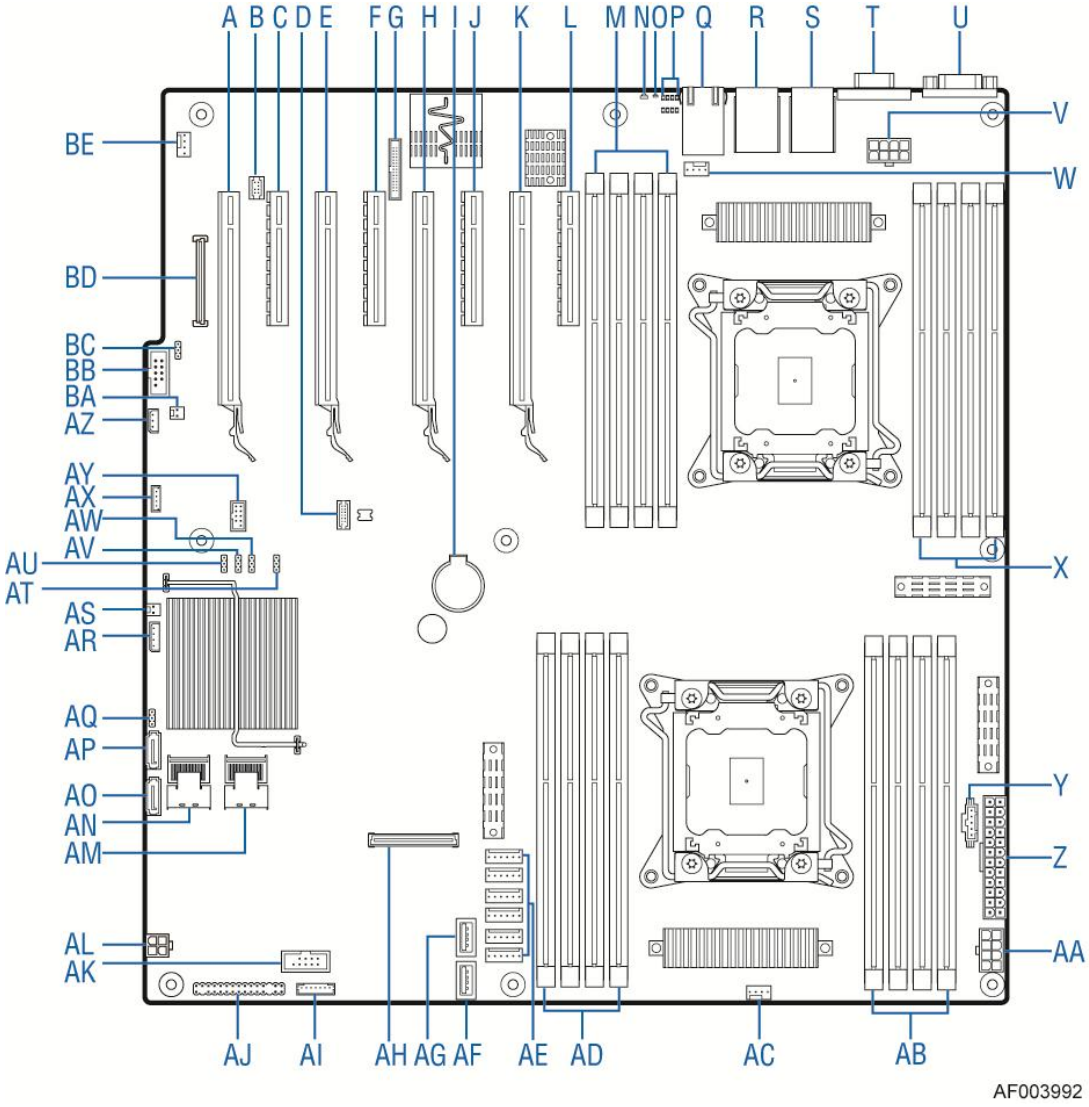
Table 1. Product Feature Set

Board Name	Intel® Server Board S2600IP	Intel® Workstation Board W2600CR
Processors	▪ Support for one or two Intel® Xeon® E5-2600 Processor(s) ▪ 8 GT/s Intel® Quick Path Interconnect (Intel® QPI) ▪ LGA 2011 Socket ▪ Thermal Design Power up to 135 W	▪ Support for one or two Intel® Xeon® E5-2600 Processor(s) ▪ 8 GT/s Intel® Quick Path Interconnect (Intel® QPI) ▪ LGA 2011 Socket ▪ Thermal Design Power up to 150 W
Chipset	Intel® C600-A chipset with support for optional Intel® C600 RAID Upgrade Keys	
Memory	▪ 16 DDR3 DIMMs with 800MT/s, 1067MT/s, 1333MT/s,1600MT/s ▪ Eight memory channels (four channels for each processor socket) ▪ Channels A, B, C, D, E, F, G and H ▪ Support for 800/1066/1333/1600 MHz/s Registered DDR3 Memory (RDIMM), ▪ Unbuffered DDR3 memory ((UDIMM) and Load Reduced DDR3 memory (LRDIMM) ▪ DDR3 standard I/O voltage of 1.5V and DDR3 Low Voltage of 1.35V	
Slots	▪ Slot 1: PCIe Gen3 x16, connector from first processor. ▪ Slot 2: PCIe Gen3 x8, connector from first processor. ▪ Slot 3: PCIe Gen3 x16, connector from first processor. ▪ Slot 4: PCIe Gen3 x8, connector from second processor. ▪ Slot 5: PCIe Gen3 x16, connector from second processor. ▪ Slot 6: PCIe Gen3 x8, connector, from second processor ▪ Slot 7: PCIe Gen3 x16,connector, from second processor ▪ Slot 8: PCIe Gen2 x4 electrical with x8 physical connector, from second processor IOM Connector: I/O Module (optional with Flex Cable) Notes: The IOM connector is not available for all boards SM Conn: SAS Module (optional) ▪ 6Gbps or 12Gbps SAS ROC module Options	
Ethernet	Intel® I350 Quad 1GbE fully integrated GbE MAC and PHY Network Controller	Intel® I350 Dual 1GbE fully integrated GbE MAC and PHY Controller
On-board storage controllers and options	▪ One eUSB 2x5 pin connector to support 2mm low-profile eUSB solid state devices ▪ Two 7-pin single port AHCI SATA connectors capable of supporting up to 6 GB/sec ▪ Two SCU 4-port mini-SAS connectors capable of supporting up to 3 GB/sec SAS/SATA ▪ Intel® Integrated RAID module support (Optional) ▪ Intel® RAID C600 Upgrade Key support providing optional expanded SATA/SAS RAID capabilities	
Video	▪ Integrated Matrox* G200 2D Video Graphics controller ▪ 1 Rear VGA port	▪ Integrated Matrox* G200 2D Video Graphics controller ▪ 1 Internal VGA connector

Board Name	Intel® Server Board S2600IP	Intel® Workstation Board W2600CR
Audio	None	ALC889 HD Audio (7.1 + S/PDIF Out)
I/O	▪ 4 Rear USB2.0 1 Rear Serial A ▪ 2 Type A USB2.0 Connectors ▪ 1 Internal Serial B	▪ 4 Rear USB2.0 2 Rear USB3.0 ▪ 2 Type A USB2.0 Connector ▪ 1 1394b Connector ▪ 1 Internal Serial B
Server Management	▪ Onboard Server Engines* LLC Pilot III* Controller ▪ Support for Intel® Remote Management Module 4 solutions ▪ Intel® Light-Guided Diagnostics on field replaceable units ▪ Support for Intel® System Management Software ▪ Support for Intel® Intelligent Power Node Manager (Need PMBus-compliant power supply)	
Security	Intel® Trusted Platform Module (TPM) - AXXTPME5 (accessory option)	
Power-Supply	750W/1200W/1600W Common Redundant Power-Supply with PMBus Support	
Suspend to RAM (S3)	NONE	Supported
Form Factor	Custom 14.2”W x 15.0”D	
Chassis	Pedestal: P4000L chassis 2U Rack: R2000 chassis	Pedestal: P4000L WS chassis

2.1.1 Main Board Connector and Component Layout

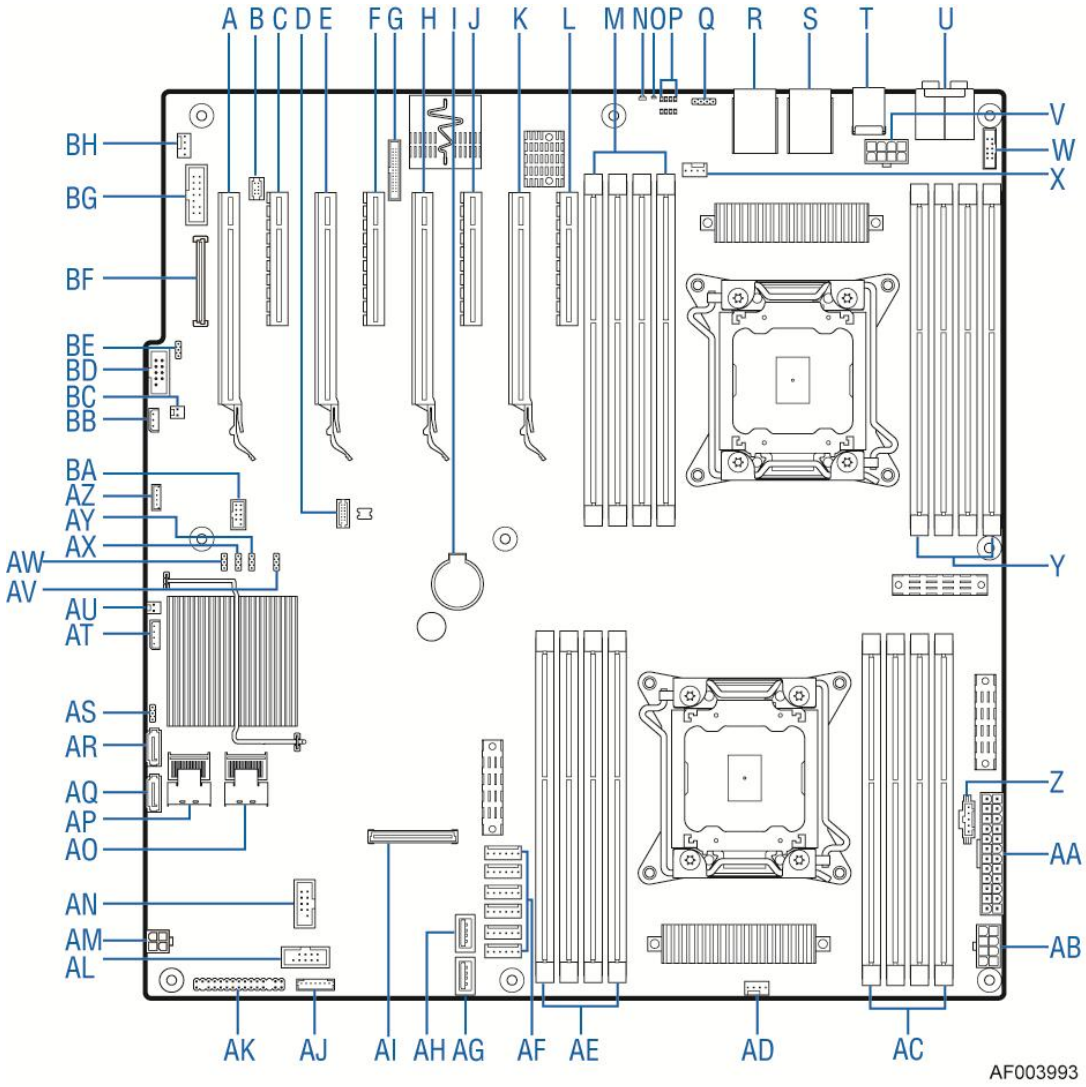
The following figure shows the layout of the server board. Each connector and major component is identified by a number or letter, and a description is given below the figure.



Callout	Description	Callout	Description
A	Slot 1, PCI Express* Gen3	AD	DIMM C1/C2/D1/D2
B	RMM4 lite module connector	AE	System Fan connector 1/2/3/4/5/6
C	Slot 2, PCI Express* Gen3	AF	Type A USB connector
D	TPM	AG	Type A USB connector
E	Slot 3, PCI Express* Gen3	AH	ROC Module connector
F	Slot 4, PCI Express* Gen3	AI	LCP connector
G	RMM4 Connector	AJ	Front Panel connector
H	Slot 5, PCI Express* Gen3	AK	Front Panel USB connector
I	Battery	AL	Main Power 4-pin connector
J	Slot 6, PCI Express* Gen3	AM	MinISAS Port B(4-7)
K	Slot 7, PCI Express* Gen3	AN	MiniSAS Port A(0-3)

Callout	Description	Callout	Description
L	Slot 8, PCI Express* Gen2	AO	SATA Port 1
M	DIMM E1/E2/F1/F2	AP	SATA Port 0
N	Status LED	AQ	CPLD Update
O	ID LED	AR	IPMB
P	Diagnostic LED	AS	HDD LED
Q	NIC 3/4 (S2600IP only)	AT	ME FRC UPDT
R	USB 2/3, NIC 2	AU	CMOS CLR
S	USB 0/1, NIC 1	AV	BIOS RCVRY
T	VGA Port (S2600IP only)	AW	PASSWD CLR
U	Serial Port A (S2600IP only)	AX	Storage Upgrade Key
V	Processor 2 Power connector	AY	eUSB SSD
W	Processor 2 Fan connector	AZ	HSBP connector
X	DIMM H2/H1/G2/G1	BA	Chassis intrusion
Y	PMBus connector	BB	Serial B connector
Z	Main Power connector	BC	BMC Force Update
AA	Processor 1 Power connector	BD	I/O Module connector (not available for S2600IP4L)
AB	DIMM B2/B1/A2/A1	BE	System Fan connector 7
AC	Processor 1 Fan connector		

Figure 3. Intel® Server Board S2600IP Major Components



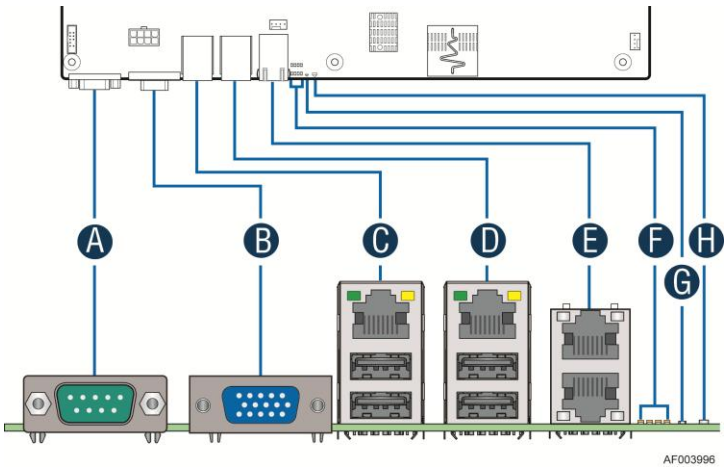
Callout	Description	Callout	Description
A	Slot 1, PCI Express* Gen3	AE	DIMM C1/C2/D1/D2
B	RMM4 Lite module	AF	System Fan connector 1/2/3/4/5/6
C	Slot 2, PCI Express* Gen3	AG	Type A USB connector
D	TPM	AH	Type A USB connector
E	Slot 3, PCI Express* Gen3	AI	ROC Module connector
F	Slot 4, PCI Express* Gen3	AJ	LCP connector
G	RMM4 Connector	AK	Front Panel connector
H	Slot 5, PCI Express* Gen3	AL	Front Panel USB connector
I	Battery	AM	Main Power 4-pin connector
J	Slot 6, PCI Express* Gen3	AN	1394b connector(W2600CR only)
K	Slot 7, PCI Express* Gen3	AO	MiniSAS Port B(4-7)
L	Slot 8, PCI Express* Gen2	AP	MiniSAS Port A(0-3)
M	DIMM E1/E2/F1/F2	AQ	SATA Port 1
N	Status LED	AR	SATA Port 0
O	ID LED	AS	CPLD Update
P	Diagnostic LED	AT	IPMB

Callout	Description	Callout	Description
Q	SPDIF connector	AU	HDD LED
R	USB 2/3, NIC 2	AV	ME FRC UPDT
S	USB 0/1, NIC 1	AW	CMOS CLR
T	USB3.0 0/1(W2600CR only)	AX	BIOS RCVRY
U	HD Audio (W2600CR only)	AY	PASSWD CLR
V	Processor 2 Power connector	AZ	Storage Upgrade Key
W	Front Audio connector	BA	eUSB SSD
X	Processor 2 Fan connector	BB	HSBP connector
Y	DIMM H2/H1/G2/G1	BC	Chassis intrusion
Z	PMBus connector	BD	Serial B connector
AA	Main Power connector	BE	BMC Force Update
AB	Processor 1 Power connector	BF	I/O Module connector (not available for W2600CR2L)
AC	DIMM B2/B1/A2/A1	BG	Internal video connector
AD	Processor 1 Fan connector	BH	System Fan connector 7

Figure 3. Intel® Workstation Board W2600CR Major Components

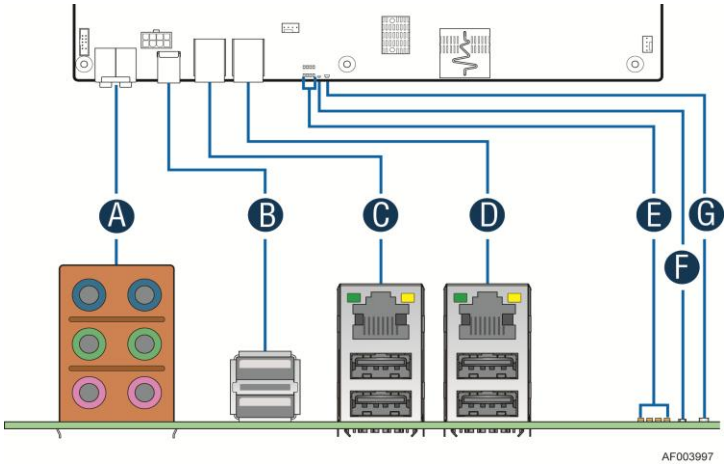
2.1.2 Main Board Rear I/O Layout

The following drawing shows the layout of the rear I/O components for the server boards.



Callout	Description	Callout	Description
A	Serial Port A	E	NIC Port 3(top) and 4(bottom)
B	Video Port	F	Diagnostics LED's
C	NIC Port 1, USB Port 0 (bottom) and 1 (top)	G	ID LED
D	NIC Port 2, USB Port 2 (bottom) and 3 (top)	H	Status LED

Figure 4. Intel® Server Board S2600IP Rear I/O Layout



Callout	Description	Callout	Description
A	7.1 Channel HD Audio Jack Connector	E	Diagnostics LED's
B	USB3.0 Port 0(bottom) and 1(top)	F	ID LED
C	NIC Port 1, USB Port 0 (bottom) and 1 (top)	G	Status LED
D	NIC Port 2, USB Port 2 (bottom) and 3 (top)		

Figure 5. Intel® Workstation Board W2600CR Rear I/O Layout

2.1.3 Server Board Mechanical Drawings

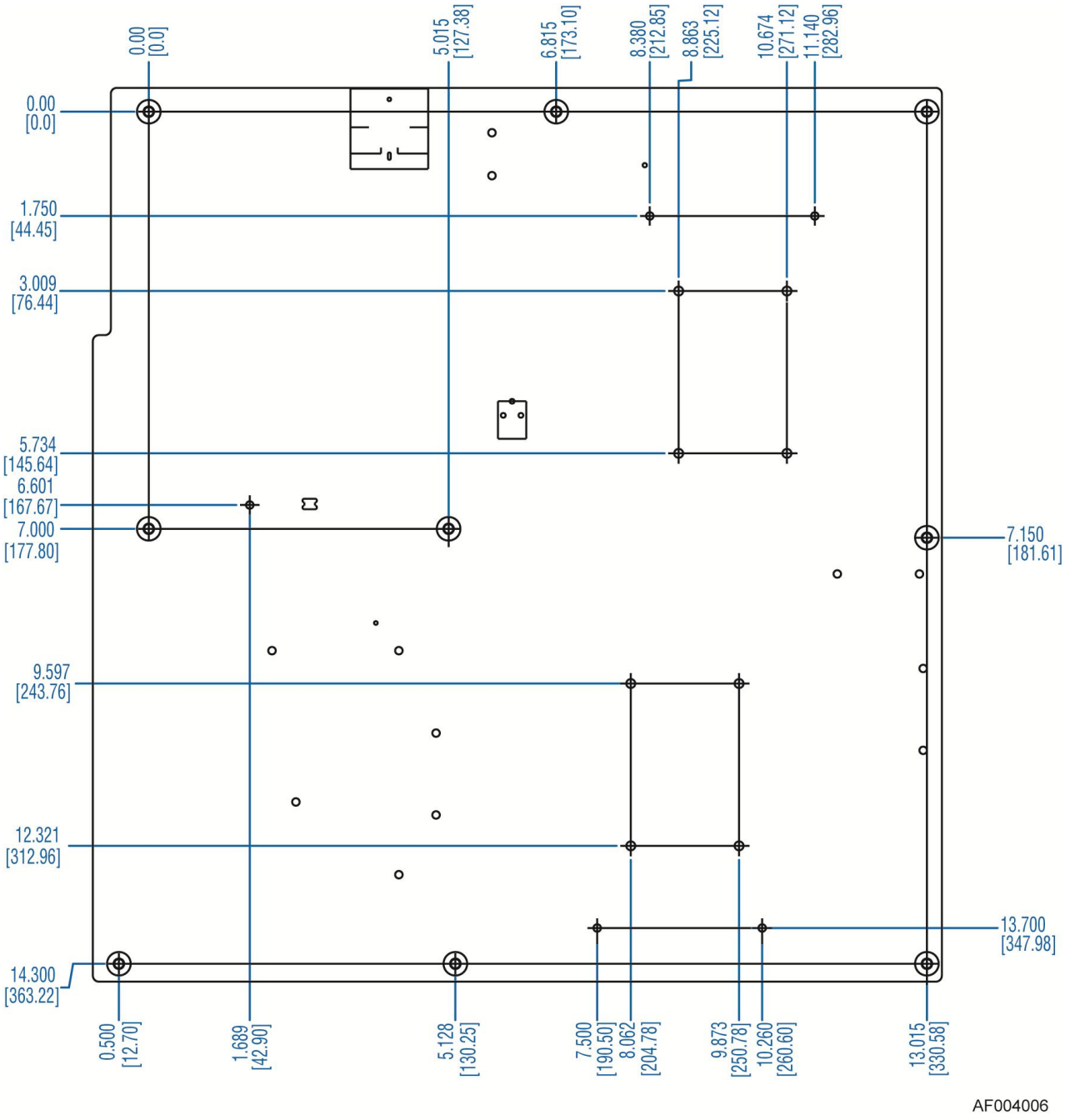


Figure 6. Mounting Hole Locations (1 of 2)

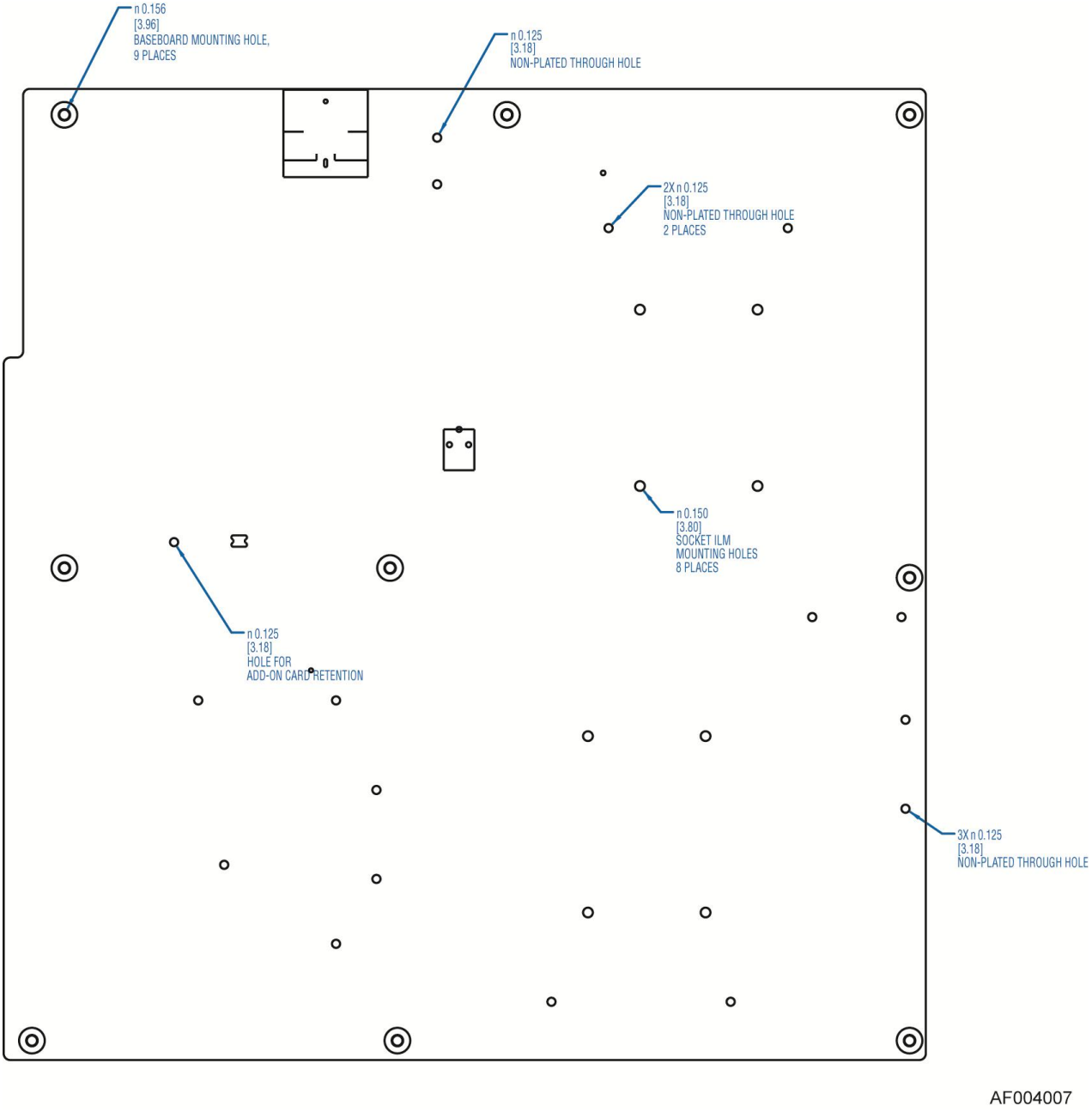


Figure 7. Mounting Hole Locations (2 of 2)

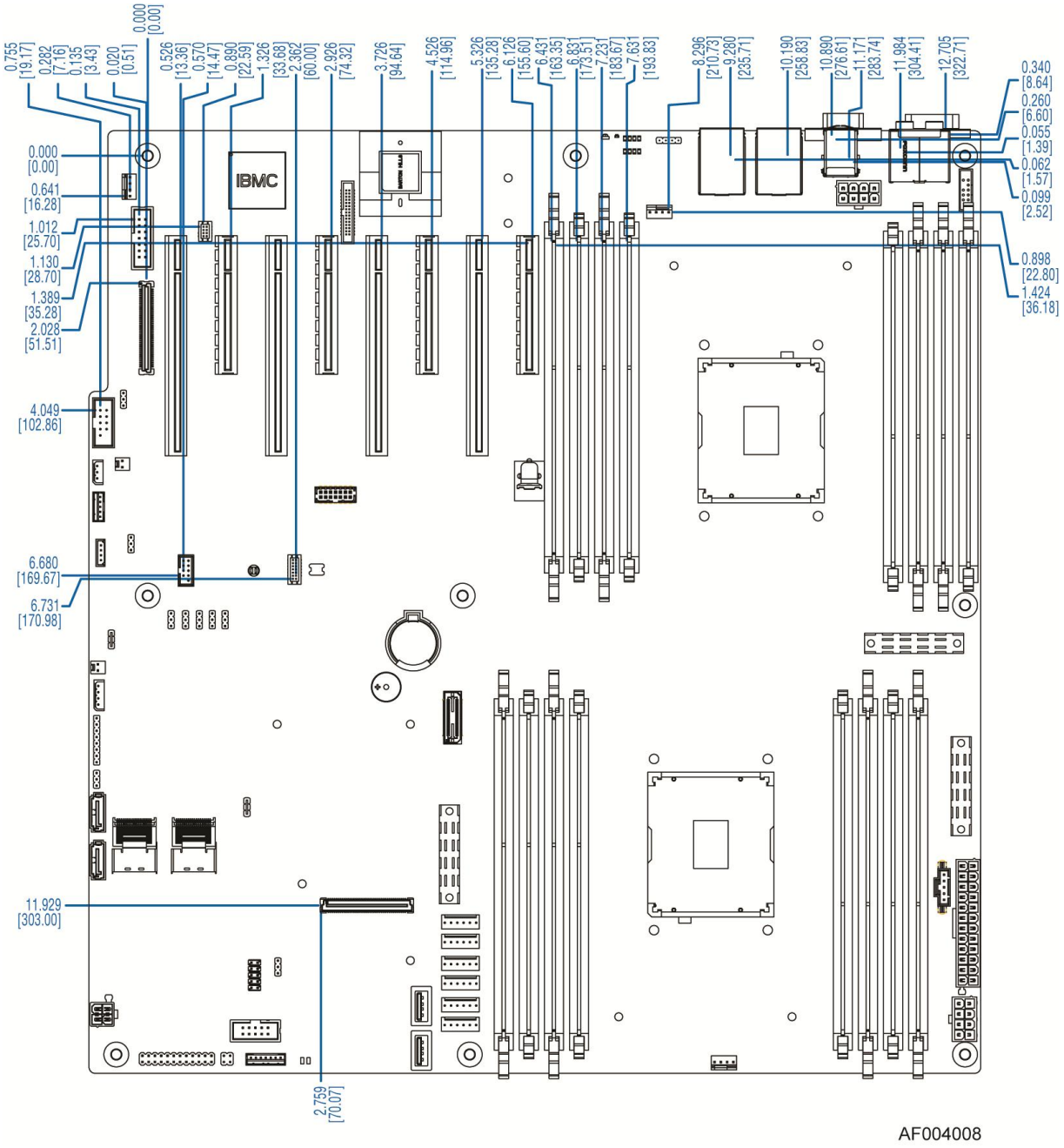


Figure 8. Major Connector Pin-1 Locations (1 of 3)

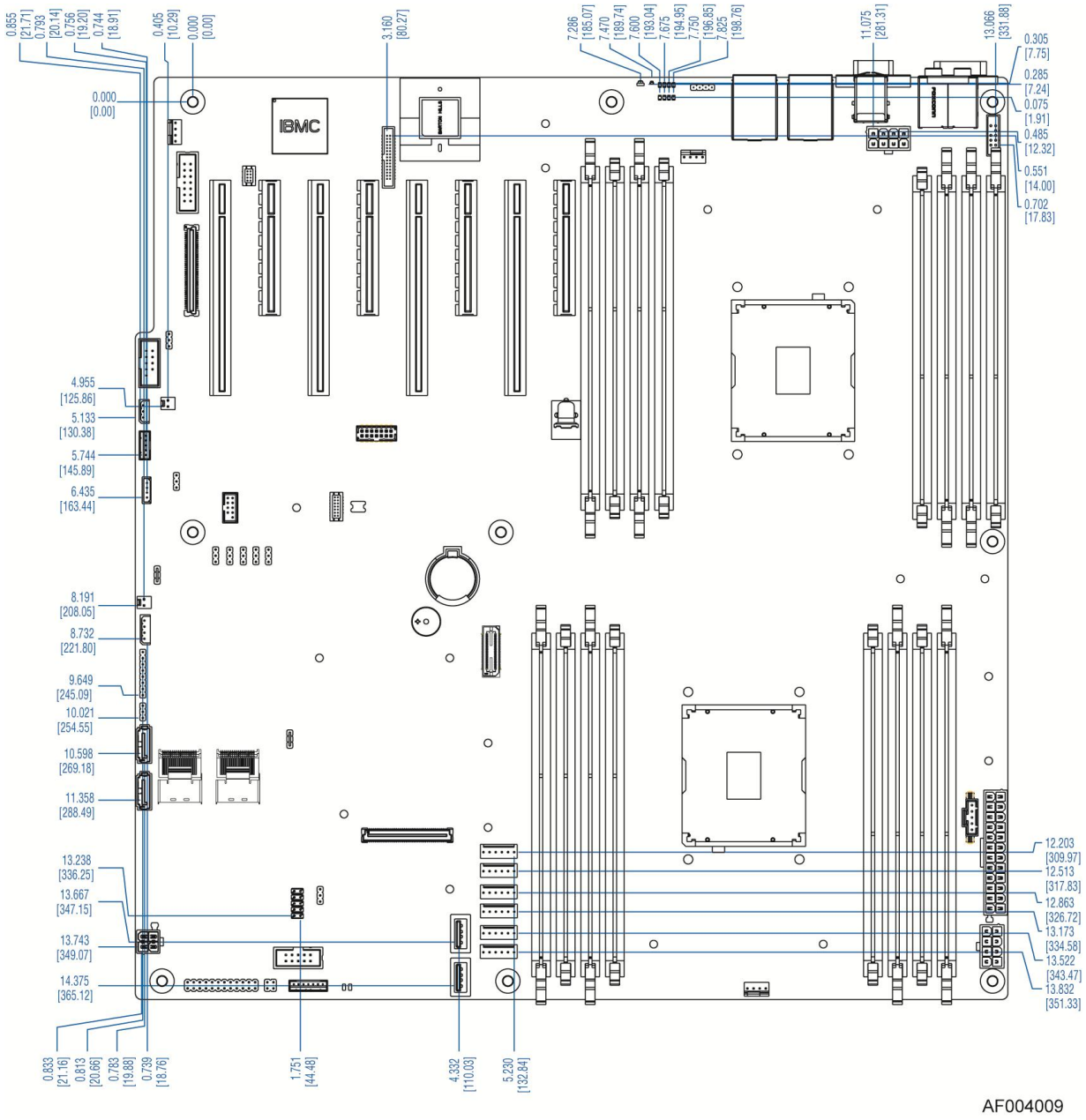


Figure 9. Major Connector Pin-1 Locations (2 of 3)

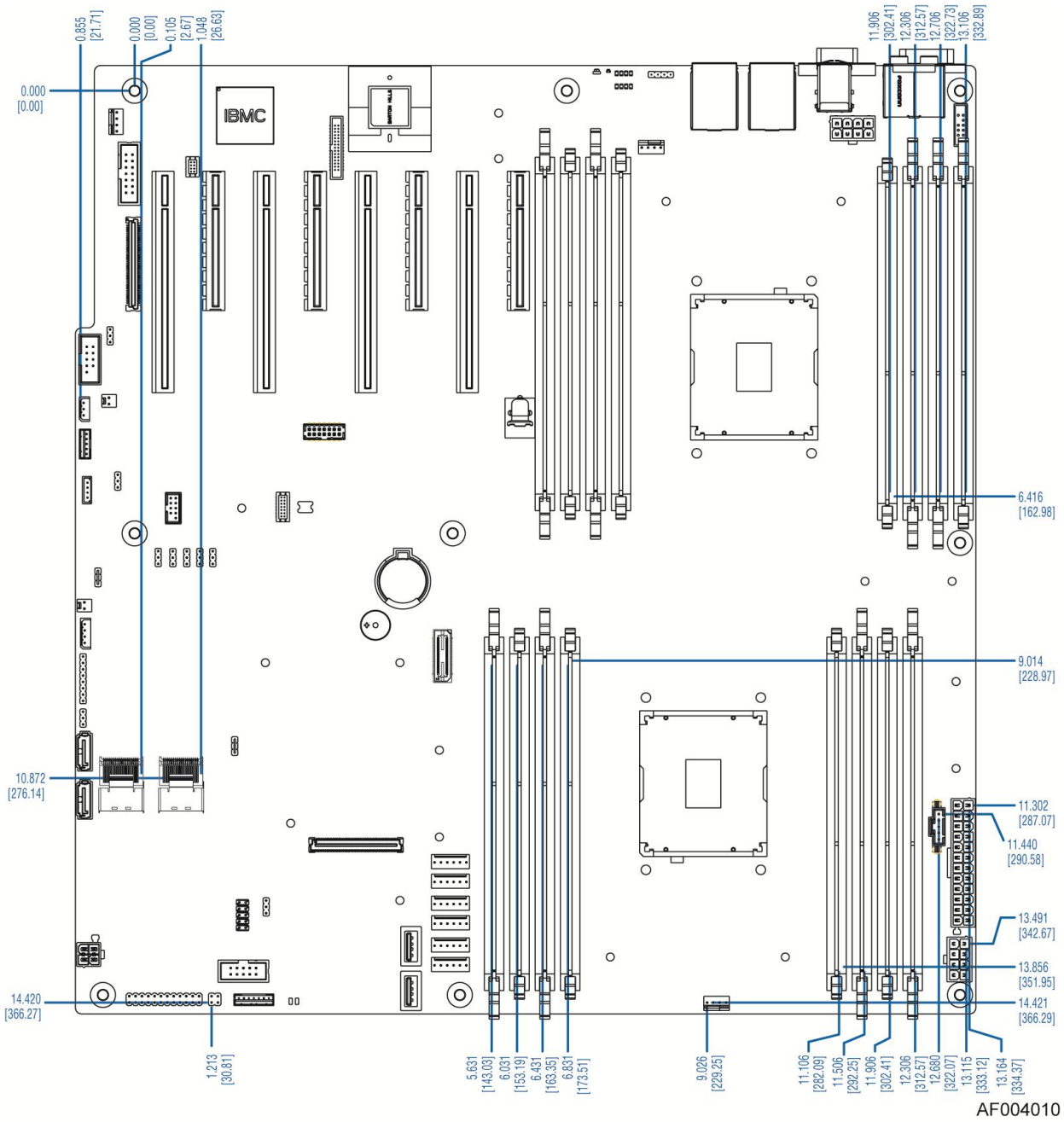
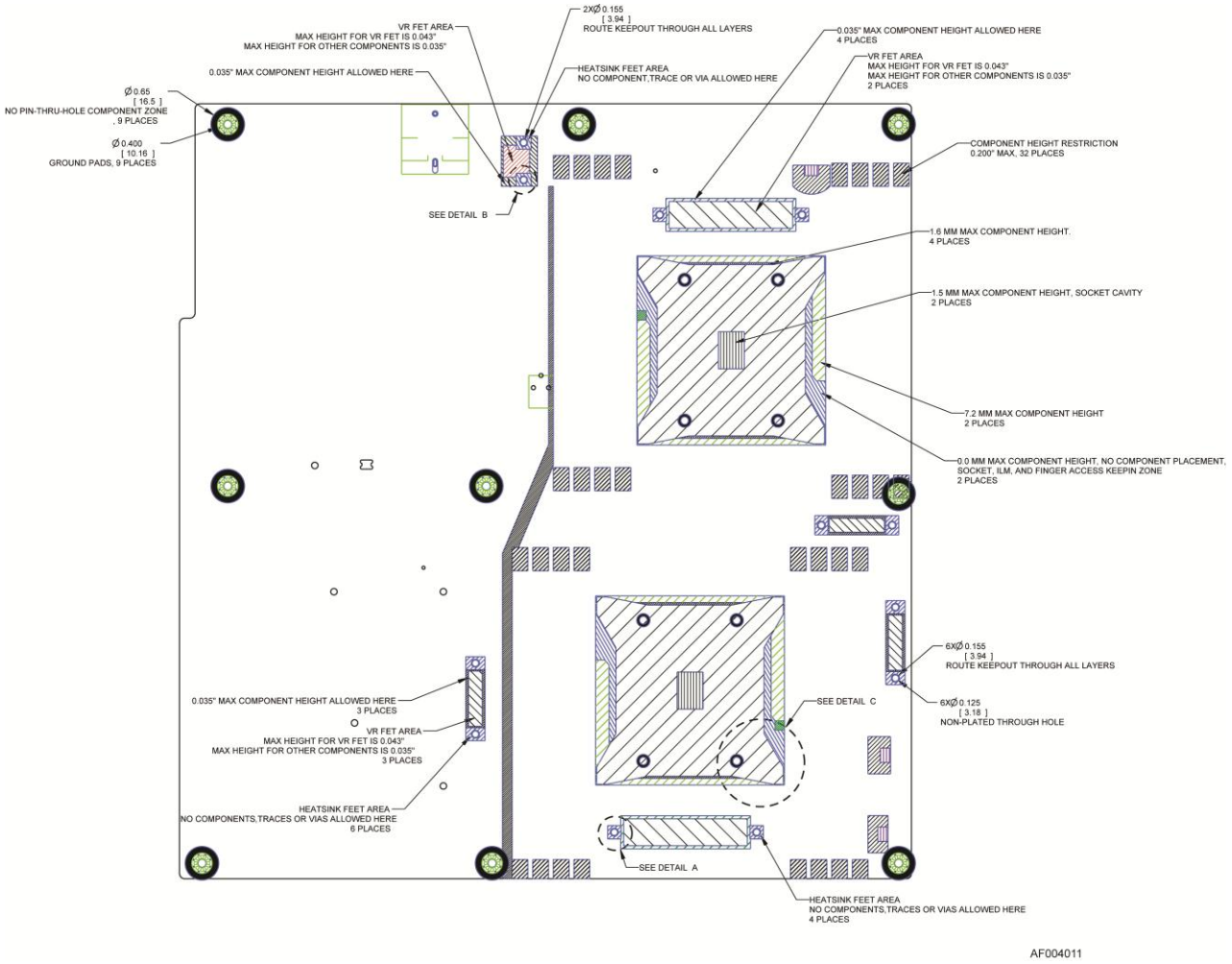
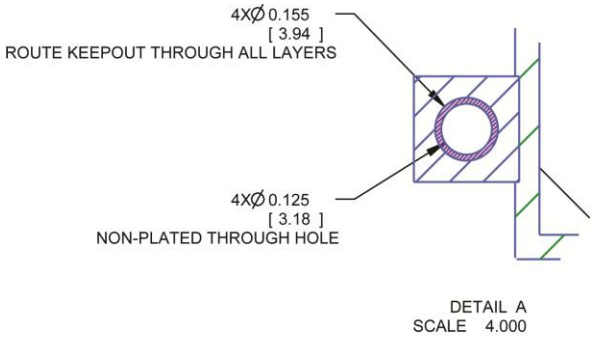
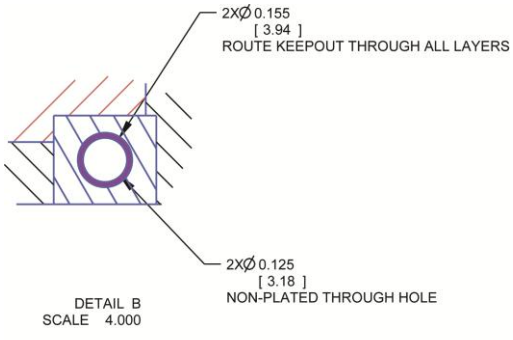


Figure 10. Major Connector Pin-1 Locations (3 of 3)


2XØ 0.155
[3.94]
ROUTE KEEPOUT THROUGH ALL LAYERS
VR FET AREA
MAX HEIGHT FOR VR FET IS 0.043"
MAX HEIGHT FOR OTHER COMPONENTS IS 0.035"
0.035" MAX COMPONENT HEIGHT ALLOWED HERE
HEATSINK FEET AREA
NO COMPONENT,TRACE OR VIA ALLOWED HERE
0.035" MAX COMPONENT HEIGHT ALLOWED HERE
4 PLACES
VR FET AREA
MAX HEIGHT FOR VR FET IS 0.043"
MAX HEIGHT FOR OTHER COMPONENTS IS 0.035"
2 PLACES
Ø 0.65
[16.5]
NO PIN-THRU-HOLE COMPONENT ZONE
, 9 PLACES
Ø 0.400
[10.16]
GROUND PADS, 9 PLACES
COMPONENT HEIGHT RESTRICTION
0.200" MAX, 32 PLACES
SEE DETAIL B
1.6 MM MAX COMPONENT HEIGHT.
4 PLACES
1.5 MM MAX COMPONENT HEIGHT, SOCKET CAVITY
2 PLACES
7.2 MM MAX COMPONENT HEIGHT
2 PLACES
0.0 MM MAX COMPONENT HEIGHT, NO COMPONENT PLACEMENT,
SOCKET, ILM, AND FINGER ACCESS KEEPIN ZONE
2 PLACES
6XØ 0.155
[3.94]
ROUTE KEEPOUT THROUGH ALL LAYERS
6XØ 0.125
[3.18]
NON-PLATED THROUGH HOLE
SEE DETAIL C
0.035" MAX COMPONENT HEIGHT ALLOWED HERE
3 PLACES
VR FET AREA
MAX HEIGHT FOR VR FET IS 0.043"
MAX HEIGHT FOR OTHER COMPONENTS IS 0.035"
3 PLACES
HEATSINK FEET AREA
NO COMPONENTS,TRACES OR VIAS ALLOWED HERE
6 PLACES
SEE DETAIL A
HEATSINK FEET AREA
NO COMPONENTS,TRACES OR VIAS ALLOWED HERE
4 PLACES
AF004011


4XØ 0.155
[3.94]
ROUTE KEEPOUT THROUGH ALL LAYERS
4XØ 0.125
[3.18]
NON-PLATED THROUGH HOLE
DETAIL A
SCALE 4.000
AF004012


2XØ 0.155
[3.94]
ROUTE KEEPOUT THROUGH ALL LAYERS
2XØ 0.125
[3.18]
NON-PLATED THROUGH HOLE
DETAIL B
SCALE 4.000
AF004013

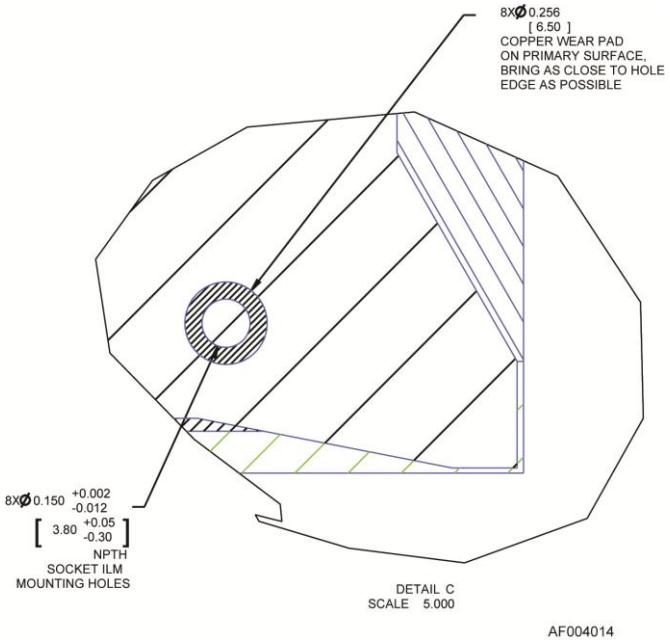


Figure 11. Primary Side Keep-out Zone

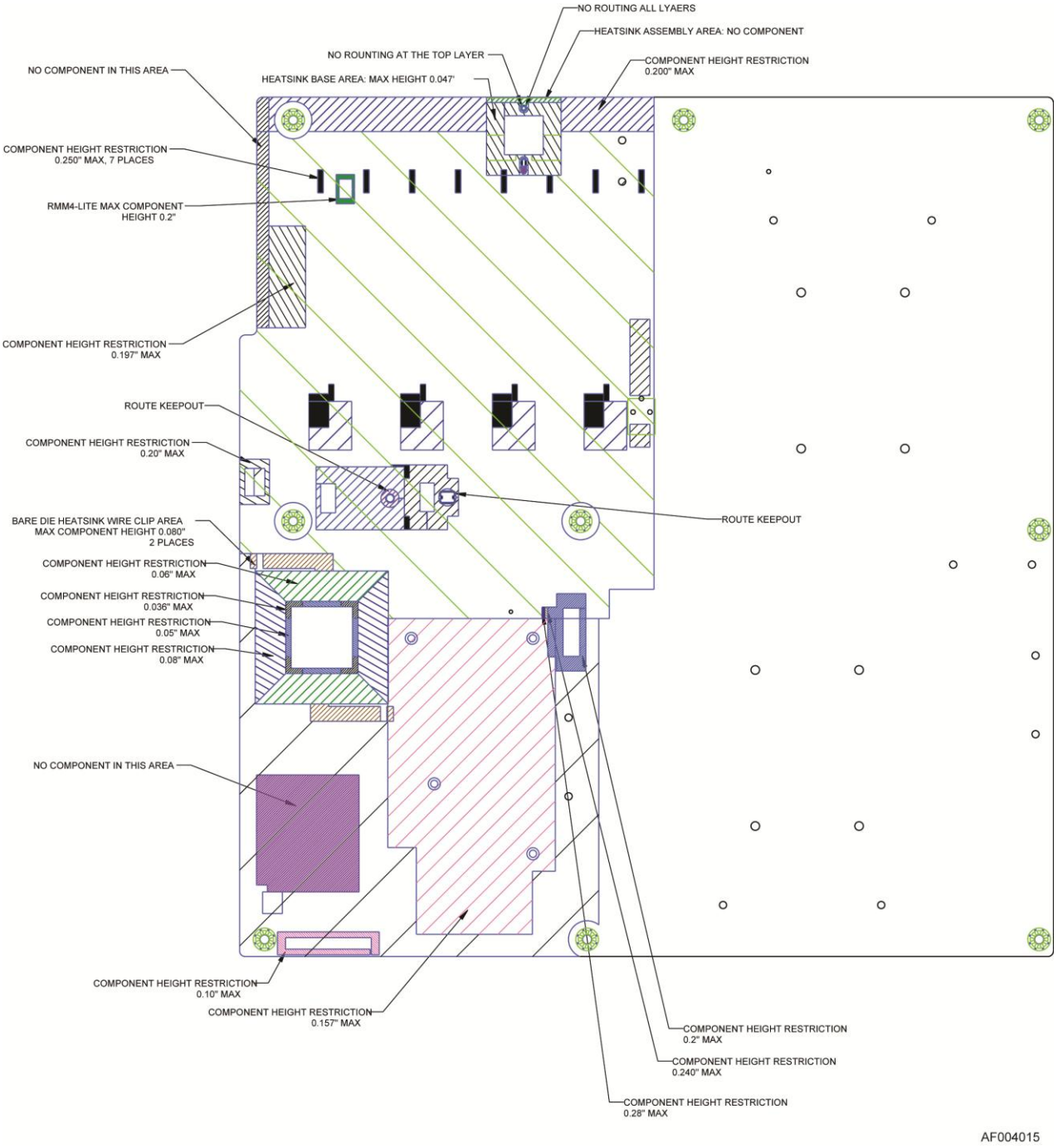


Figure 12. Primary Side Card-Side Keep-out Zone

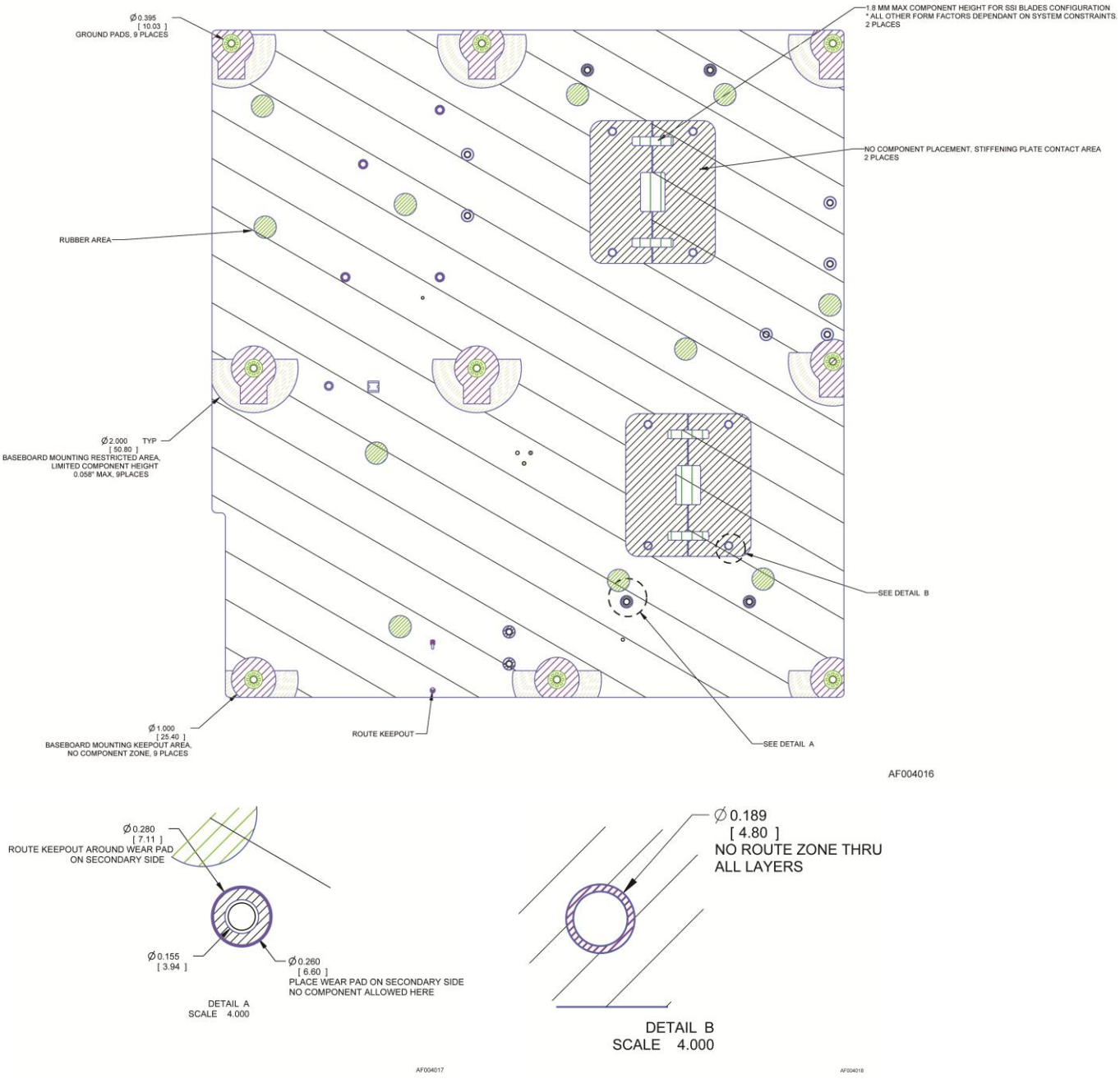


Figure 13. Second Side Keep-out Zone

3. Functional Architecture

The architecture and design of the Intel® Server Board S2600IP and Intel® Workstation Board W2600CR is based on the Intel® C600-A chipset. The chipset is designed for systems based on the Intel® Xeon® Sandy Bridge-EP Processor series in an LGA 2011 Socket with Intel® Quick Path Interconnect (Intel® QPI) speed at 8GT/s.

This chapter provides a high-level description of the functionality associated with each chipset component and the architectural blocks that make up the server boards.

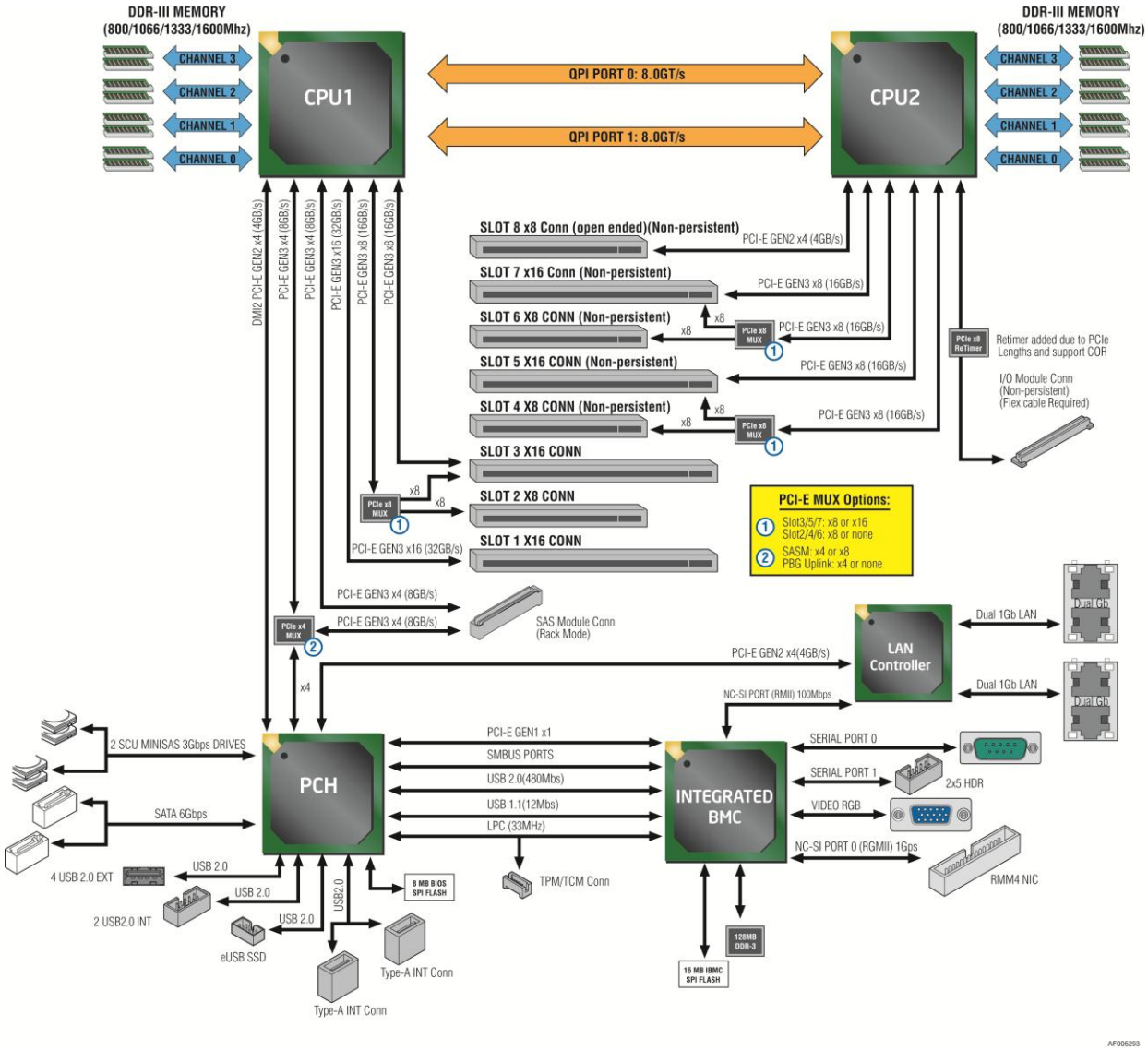


Figure 14. Intel® Server Board S2600IP Functional Block Diagram

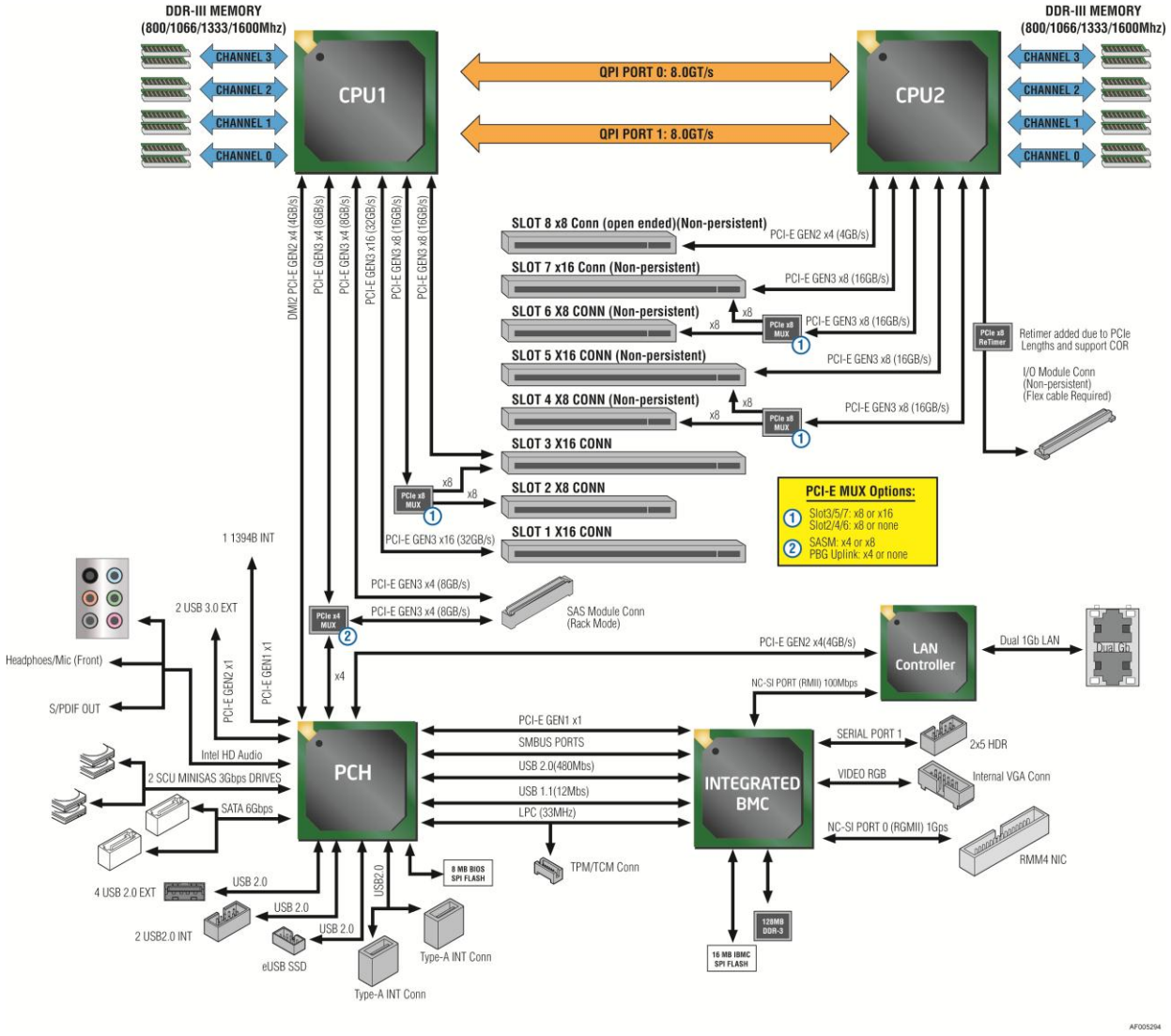


Figure 15. Intel® Workstation Board W2600CR Functional Block Diagram

3.1 Processor Support

The server board includes two Socket-R (LGA2011) processor sockets and can support one or two of the following processors - Intel® Xeon® processor E5-2600 product family with a Thermal Design Power (TDP) of up to 150w.

Note: The 150w TDP processors only supported on Intel® Workstation Board W2600CR and Intel® Server Board S2600IP only support update to 135w TDP processors. Previous generation Intel® Xeon® processors are not supported on the Intel server boards described in this document.

For a complete updated list of supported processors, please visit the support website.

3.1.1 Processor Socket Assembly

Each processor socket of the server board is pre-assembled with an Independent Latching Mechanism (ILM) and Back Plate which allow for secure placement of the processor and processor heat to the server board. The illustration below identifies each sub-assembly component.

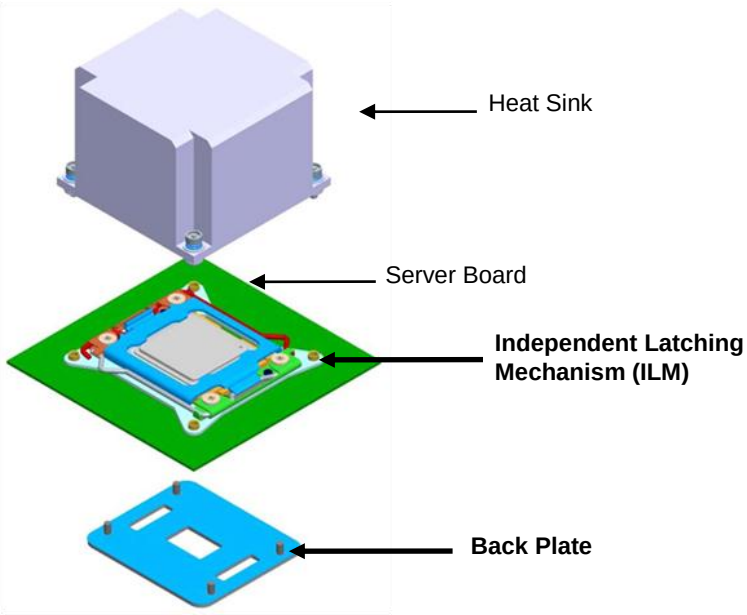


Figure 16. Processor Socket Assembly

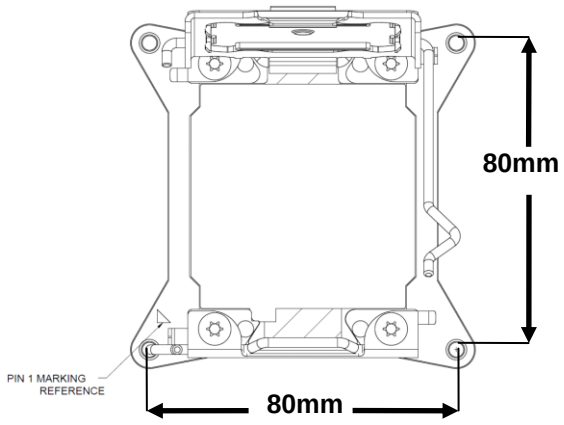


Figure 17. Processor Socket ILM

The square ILM has an 80x80mm heat sink mounting hole pattern and is used on the Intel® Server Board S2600IP and Intel® Workstation Board W2600CR.

Note: Processor Thermal solutions for the Intel® Workstation Board W2600CR are NOT the same with Intel® Server Board S2600IP when install 150W TDP Processors.

3.1.2 Processor Population Rules

Note: Although the server board does support dual-processor configurations consisting of different processors that meet the defined criteria below, Intel does not perform validation testing of this configuration. For optimal system performance in dual-processor configurations, Intel recommends that identical processors be installed.

When using a single processor configuration, the processor must be installed into the processor socket labeled “CPU_1”.

When two processors are installed, the following population rules apply:

- Both processors must be of the same processor family.
- Both processors must have the same number of cores.
- Both processors must have the same cache sizes for all levels of processor cache memory.
- Processors with different core frequencies can be mixed in a system, given the prior rules are met. If this condition is detected, all processor core frequencies are set to the lowest common denominator (highest common speed) and an error is reported.
- Processors which have different QPI link frequencies may operate together if they are otherwise compatible and if a common link frequency can be selected. The common link frequency would be the highest link frequency that all installed processors can achieve.
- Processor stepping within a common processor family can be mixed as long as it is listed in the processor specification updates published by Intel Corporation.

3.1.3 Processor Initialization Error Summary

The following table describes mixed processor conditions and recommended actions for all Intel® server boards and Intel server systems designed around the Intel® Xeon® processor E5-2600 product family and Intel® C600 chipset product family architecture. The errors fall into one of the following three categories:

- **Fatal:** If the system can boot, it pauses at a blank screen with the text **“Unrecoverable fatal error found. System will not boot until the error is resolved”** and **“Press <F2> to enter setup”**, regardless of whether the “Post Error Pause” setup option is enabled or disabled.

  When the operator presses the <F2> key on the keyboard, the error message is displayed on the Error Manager screen, and an error is logged to the System Event Log (SEL) with the POST Error Code.

  The system cannot boot unless the error is resolved. The user needs to replace the faulty part and restart the system.

  For Fatal Errors during processor initialization, the System Status LED will be set to a steady Amber color, indicating an unrecoverable system failure condition.

- **Major:** If the "Post Error Pause" setup option is enabled, the system goes directly to the Error Manager to display the error, and logs the POST Error Code to SEL. Operator intervention is required to continue booting the system.

  Otherwise, if "POST Error Pause" is disabled, the system continues to boot and no prompt is given for the error, although the Post Error Code is logged to the Error Manager and in a SEL message.

- **Minor:** The message is displayed on the screen or on the Error Manager screen, and the POST Error Code is logged to the SEL. The system continues booting in a degraded state. The user may want to replace the erroneous unit. The POST Error Pause option setting in the BIOS setup does not have any effect on this error.

Table 2. Mixed Processor Configurations Error Summary.

Error	Severity	System Action
Processor family not Identical	Fatal	The BIOS detects the error condition and responds as follows: ▪ Logs the POST Error Code into the System Event Log (SEL). ▪ Alerts the BMC to set the System Status LED to steady Amber. ▪ Displays "***0194: Processor family mismatch detected***" message in the Error Manager. ▪ Takes Fatal Error action (see above) and will not boot until the fault condition is remedied.
Processor model not Identical	Fatal	The BIOS detects the error condition and responds as follows: ▪ Logs the POST Error Code into the System Event Log (SEL). ▪ Alerts the BMC to set the System Status LED to steady Amber. ▪ Displays "***0196: Processor model mismatch detected***" message in the Error Manager. ▪ Takes Fatal Error action (see above) and will not boot until the fault condition is remedied.
Processor cores/threads not identical	Fatal	The BIOS detects the error condition and responds as follows: ▪ Logs the POST Error Code into the SEL. ▪ Alerts the BMC to set the System Status LED to steady Amber. ▪ Displays "***0191: Processor core/thread count mismatch detected***" message in the Error Manager. Takes Fatal Error action (see above) and will not boot until the fault condition is remedied.
Processor cache not identical	Fatal	The BIOS detects the error condition and responds as follows: ▪ Logs the POST Error Code into the SEL. ▪ Alerts the BMC to set the System Status LED to steady Amber. ▪ Displays "***0192: Processor cache size mismatch detected*** message in the Error Manager. ▪ Takes Fatal Error action (see above) and will not boot until the fault condition is remedied.

Error	Severity	System Action
Processor frequency (speed) not identical	Fatal	The BIOS detects the processor frequency difference, and responds as follows: ▪ Adjusts all processor frequencies to the highest common frequency. ▪ No error is generated – **this is not an error condition.** ▪ Continues to boot the system successfully. If the frequencies for all processors **cannot be adjusted to be the same,** then this ***is*** an error, and the BIOS responds as follows: ▪ Logs the POST Error Code into the SEL. ▪ Alerts the BMC to set the System Status LED to steady Amber. ▪ Does not disable the processor. ▪ Displays "***0197: Processor speeds unable to synchronize***" message in the Error Manager. ▪ Takes Fatal Error action (see above) and will not boot until the fault condition is remedied.
Processor Intel® QuickPath Interconnect link frequencies not identical	Fatal	The BIOS detects the QPI link frequencies and responds as follows: ▪ Adjusts all QPI interconnect link frequencies to highest common frequency. ▪ No error is generated – **this is not an error condition.** ▪ Continues to boot the system successfully. If the link frequencies for all QPI links **cannot be adjusted to be the same,** then this ***is*** an error, and the BIOS responds as follows: ▪ Logs the POST Error Code into the SEL. ▪ Alerts the BMC to set the System Status LED to steady Amber. ▪ Displays "***0195: Processor Intel(R) QPI link frequencies unable to synchronize***" message in the Error Manager. ▪ Does not disable the processor. ▪ Takes Fatal Error action (see above) and will not boot until the fault condition is remedied.
Processor microcode update missing	Minor	The BIOS detects the error condition and responds as follows: ▪ Logs the POST Error Code into the SEL. ▪ Displays "***818x: Processor 0x microcode update not found***" message in the Error Manager or on the screen. ▪ The system continues to boot in a degraded state, regardless of the setting of POST Error Pause in the Setup.
Processor microcode update failed	Major	The BIOS detects the error condition and responds as follows: ▪ Logs the POST Error Code into the SEL. ▪ Displays "***816x: Processor 0x unable to apply microcode update***" message in the Error Manager or on the screen. Takes Major Error action. The system may continue to boot in a degraded state, depending on the setting of POST Error Pause in Setup, or may halt with the POST Error Code in the Error Manager waiting for operator intervention.

3.2 Processor Functions Overview

With the release of the Intel® Xeon® processor E5-2600 product family, several key system components, including the CPU, Integrated Memory Controller (IMC), and Integrated IO Module (IIO), have been combined into a single processor package and feature per socket; two Intel® QuickPath Interconnect point-to-point links capable of up to 8.0 GT/s, up to 40 lanes of Gen 3 PCI Express* links capable of 8.0 GT/s, and 4 lanes of DMI2/PCI Express* Gen 2 interface with a peak transfer rate of 5.0 GT/s. The processor supports up to 46 bits of physical address space and 48-bit of virtual address space.

The following sections will provide an overview of the key processor features and functions that help to define the performance and architecture of the server board. For more comprehensive processor specific information, refer to the Intel® Xeon® processor E5-2600 product family documents listed in the Reference Document list.
Processor Feature Details:

- Up to eight execution cores
- Each core supports two threads (Intel® Hyper-Threading Technology), up to 16 threads per socket
- 46-bit physical addressing and 48-bit virtual addressing
- 1 GB large page support for server applications
- A 32-KB instruction and 32-KB data first-level cache (L1) for each core
- A 256-KB shared instruction/data mid-level (L2) cache for each core
- Up to 20 MB last level cache (LLC): up to 2.5 MB per core instruction/data last level cache (LLC), shared among all cores

Supported Technologies:

- Intel® Virtualization Technology (Intel® VT)
- Intel® Virtualization Technology for Directed I/O (Intel® VT-d)
- Intel® Virtualization Technology “Sandy Bridge” Processor Extensions
- Intel® Trusted Execution Technology (Intel® TXT)
- Intel® 64 Architecture
- Intel® Streaming SIMD Extensions 4.1 (Intel® SSE4.1)
- Intel® Streaming SIMD Extensions 4.2 (Intel® SSE4.2)
- Intel® Advanced Vector Extensions (Intel® AVX)
- Intel® Hyper-Threading Technology
- Execute Disable Bit
- Intel® Turbo Boost Technology
- Intel® Intelligent Power Technology
- Enhanced Intel® SpeedStep Technology

3.2.1 Intel® QuickPath Interconnect

The Intel® QuickPath Interconnect is a high speed, packetized, point-to-point interconnect used in the processor. The narrow high-speed links stitch together processors in distributed shared memory and integrated I/O platform architecture. It offers much higher bandwidth with low latency. The Intel® QuickPath Interconnect has an efficient architecture allowing more

interconnect performance to be achieved in real systems. It has a snoop protocol optimized for low latency and high scalability, as well as packet and lane structures enabling quick completions of transactions. Reliability, availability, and serviceability features (RAS) are built into the architecture.

The physical connectivity of each interconnect link is made up of twenty differential signal pairs plus a differential forwarded clock. Each port supports a link pair consisting of two uni-directional links to complete the connection between two components. This supports traffic in both directions simultaneously. To facilitate flexibility and longevity, the interconnect is defined as having five layers: Physical, Link, Routing, Transport, and
Protocol.

The Intel® QuickPath Interconnect includes a cache coherency protocol to keep the distributed memory and caching structures coherent during system operation. It supports both low-latency source snooping and a scalable home snoop behavior. The coherency protocol provides for direct cache-to-cache transfers for optimal latency.

3.2.2 Integrated Memory Controller (IMC) and Memory Subsystem

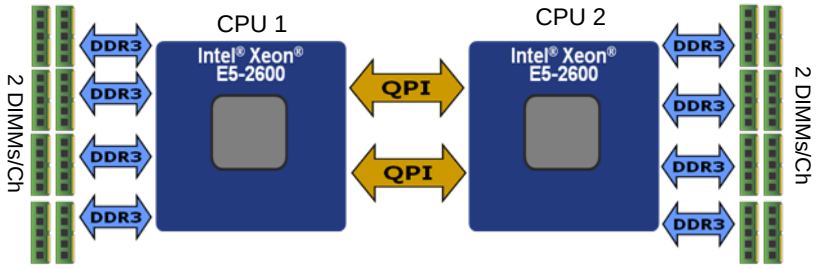


Figure 18. Integrated Memory Controller Functional Block Diagram

- Unbuffered DDR3 and registered DDR3 DIMMs
- LR DIMM (Load Reduced DIMM) for buffered memory solutions demanding higher capacity memory subsystems
- Independent channel mode or lockstep mode
- Data burst length of eight cycles for all memory organization modes
- Memory DDR3 data transfer rates of 800, 1066, 1333, and 1600 MT/s
- 64-bit wide channels plus 8-bits of ECC support for each channel
- DDR3 standard I/O Voltage of 1.5 V and DDR3 Low Voltage of 1.35 V
- 1-Gb, 2-Gb, and 4-Gb DDR3 DRAM technologies supported for these devices:
  - UDIMM DDR3 – SR x8 and x16 data widths, DR – x8 data width
  - RDIMM DDR3 – SR,DR, and QR – x4 and x8 data widths
  - LRDIMM DDR3 – QR – x4 and x8 data widths with direct map or with rank multiplication
- Up to 8 ranks supported per memory channel, 1, 2 or 4 ranks per DIMM
- Open with adaptive idle page close timer or closed page policy
- Per channel memory test and initialization engine can initialize DRAM to all logical zeros with valid ECC (with or without data scrambler) or a predefined test pattern

- Isochronous access support for Quality of Service (QoS)
- Minimum memory configuration: independent channel support with 1 DIMM populated
- Integrated dual SMBus master controllers
- Command launch modes of 1n/2n
- RAS Support:
  - Rank Level Sparing and Device Tagging
  - Demand and Patrol Scrubbing
  - DRAM Single Device Data Correction (SDDC) for any single x4 or x8 DRAM device. Independent channel mode supports x4 SDDC. x8 SDDC requires lockstep mode
  - Lockstep mode where channels 0 and 1 and channels 2 and 3 are operated in lockstep mode
  - Data scrambling with address to ease detection of write errors to an incorrect address.
  - Error reporting from Machine Check Architecture
  - Read Retry during CRC error handling checks by iMC
  - Channel mirroring within a socket
    - CPU1 Channel Mirror Pairs (A,B) and (C,D)
    - CPU2 Channel Mirror Pairs (E,F) and (G,H)
  - Error Containment Recovery
- Improved Thermal Throttling with dynamic Closed Loop Thermal Throttling (CLTT)
- Memory thermal monitoring support for DIMM temperature

3.2.2.1 Supported Memory

Table 3. UDIMM Support Guidelines

Ranks Per DIMM and Data Width	Memory Capacity Per DIMM[1]			Speed (MT/s) and Voltage Validated by Slot per Channel (SPC) and DIMM Per Channel (DPC)[2,3]			
				2 Slots per Channel			
				1DPC		2DPC	
				1.35V	1.5V	1.35V	1.5V
SRx8 Non-ECC	1GB	2GB	4GB	n/a	1066, 1333	n/a	1066, 1333
DRx8 Non-ECC	2GB	4GB	8GB	n/a	1066, 1333	n/a	1066, 1333
SRx16 Non-ECC	512MB	1GB	2GB	n/a	1066, 1333	n/a	1066, 1333
SRx8 ECC	1GB	2GB	4GB	1066,1333	1066, 1333	1066	1066, 1333
DRx8 ECC	2GB	4GB	8GB	1066,1333	1066, 1333	1066	1066, 1333

Notes:
1. Supported DRAM Densities are 1Gb, 2Gb and 4Gb. Only 2Gb and 4Gb are validated by Intel.
2. Command Address Timing is 1N for 1DPC and 2N for 2DPC.

	Supported and Validated
	Supported but not Validate

Table 4. RDIMM Support Guidelines

Ranks Per DIMM and Data Width	Memory Capacity Per DIMM[1]			Speed (MT/s) and Voltage Validated by Slot per Channel (SPC) and DIMM Per Channel (DPC)[2]			
				2 Slots per Channel			
				1DPC		2DPC	
				1.35V	1.5V	1.35V	1.5V
SRx8	1GB	2GB	4GB	1066 1333	1066 1333 1600	1066 1333	1066 1333 1600
DRx8	2GB	4GB	8GB	1066 1333	1066 1333 1600	1066 1333	1066 1333 1600
SRx4	2GB	4GB	8GB	1066 1333	1066 1333 1600	1066 1333	1066 1333 1600
DRx4	4GB	8GB	16GB	1066 1333	1066 1333 1600	1066 1333	1066 1333 1600
QRx4	8GB	16GB	32GB	800	1066	800	800
QRx8	4GB	8GB	16GB	800	1066	800	800

Notes:
1. Supported DRAM Densities are 1Gb, 2Gb and 4Gb. Only 2Gb and 4Gb are validated by Intel.
2. Command Address Timing is 1N.
3. QR RDIMM are supported but only validated by Intel/PMO in a homogenous environment. The coverage will have limited system level testing, no signal integrity testing, and no interoperability testing The passing QR RDIMMs will be web posted.

	Supported and Validated
	Supported but not Validate
	Supported w/Limited Validation[4]

Table 5. LRDIMM Support Guidelines

Ranks Per DIMM and Data Width[1]	Memory Capacity Per DIMM[2]		Speed (MT/s) and Voltage Validated by Slot per Channel (SPC) and DIMM Per Channel (DPC)[3,4]	
			2 Slots per Channel	
			1DPC and 2DPC	
			1.35V	1.5V
QRx4 (DDP)[5]	16GB	32GB	1066	1066, 1333
QRx8 (P)[5]	8GB	16GB	1066	1066, 1333

Notes:
1. Physical Rank is used to calculate DIMM Capacity.
2. Supported and validated DRAM Densities are 2Gb and 4Gb.
3. Command Address Timing is 1N.
4. The speeds are estimated targets and will be verified through simulation.
5. DDP - Dual Die Package DRAM stacking. P – Planer monolithic DRAM Die.

	Supported and Validated

3.2.2.2 Memory Population Rules

Note: Although mixed DIMM configurations are supported, Intel only performs platform validation on systems that are configured with identical DIMMs installed.

Each processor provides four banks of memory, each capable of supporting up to 2 DIMMs.

- DIMMs are organized into physical slots on DDR3 memory channels that belong to processor sockets.
- The memory channels from processor socket 1 are identified as Channel A, B, C and D. The memory channels from processor socket 2 are identified as Channel E, F, G, and H.
- The silk screened DIMM slot identifiers on the board provide information about the channel, and therefore the processor to which they belong. For example, DIMM_A1 is the first slot on Channel A on processor 1; DIMM_E1 is the first DIMM socket on Channel E on processor 2.
- The memory slots associated with a given processor are unavailable if the corresponding processor socket is not populated.
- A processor may be installed without populating the associated memory slots provided a second processor is installed with associated memory. In this case, the memory is shared by the processors. However, the platform suffers performance degradation and latency due to the remote memory.
- Processor sockets are self-contained and autonomous. However, all memory subsystem support (such as Memory RAS, Error Management,) in the BIOS setup are applied commonly across processor sockets.

On the Intel® Server Board S2600IP and Intel® Workstation Board W2600CR a total of 16 DIMM slots is provided (2 CPUs – 4 Channels / CPU, 2 DIMMs /Channel). The nomenclature for DIMM sockets is detailed in the following table:

Table 6. DIMM Nomenclature

Processor Socket 1								Processor Socket 2							
(0) Channel A		(1) Channel B		(2) Channel C		(3) Channel D		(0) Channel E		(1) Channel F		(2) Channel G		(3) Channel H	
A1	**A2**	**B1**	**B2**	**C1**	**C2**	**D1**	**D2**	**E1**	**E2**	**F1**	**F2**	**G1**	**G2**	**H1**	**H2**

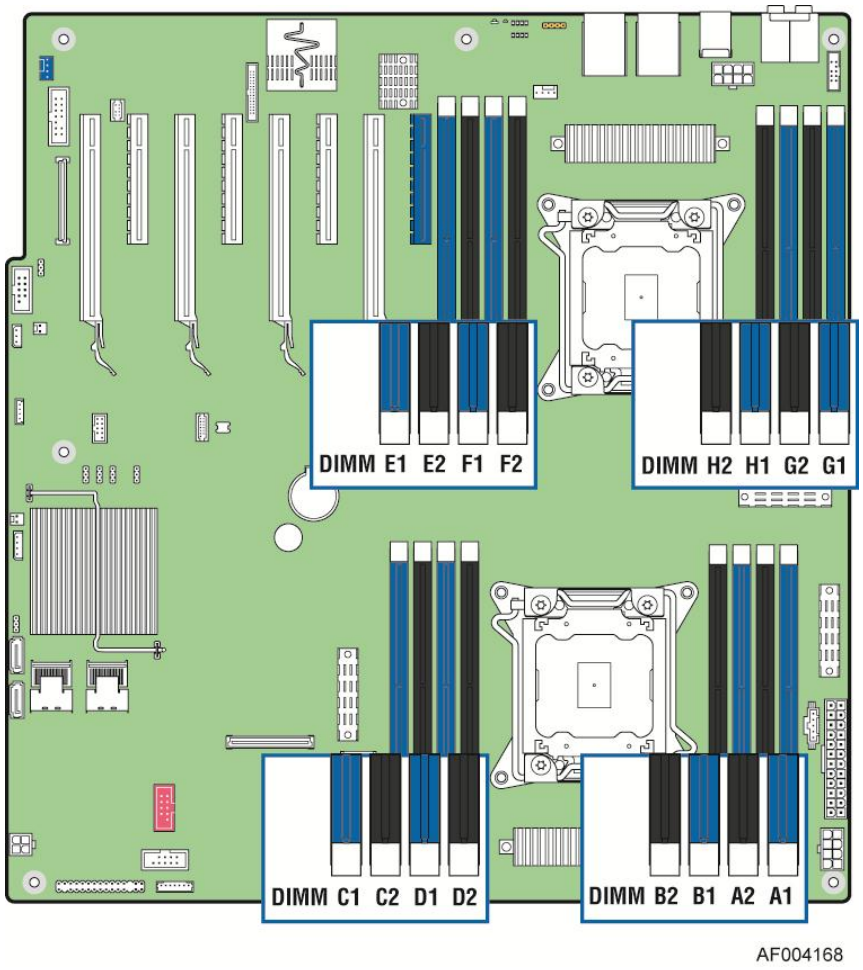


Figure 19. DIMM Slot Layout

The following are generic DIMM population requirements that generally apply to both the Intel® Server Board S2600IP and Intel® Workstation Board W2600CR.

- DIMM slots on any memory channel must be filled following the “farthest fill first” rule.
- A maximum of 8 ranks can be installed on any one channel, counting all ranks in each DIMM on the channel.
- DIMM types (UDIMM, RDIMM, LRDIMM) must not be mixed within or across processor sockets.
- Mixing ECC with non-ECC DIMMs (UDIMMs) is not supported within or across processor sockets.
- Mixing Low Voltage (1.35V) DIMMs with Standard Voltage (1.5V) DIMMs is not supported within or across processor sockets.
- Mixing DIMMs of different frequencies and latencies is not supported within or across processor sockets.
- LRDIMM Rank Multiplication Mode and Direct Map Mode must not be mixed within or across processor sockets.
- Only ECC UDIMMs support Low Voltage 1.35V operation.

- QR RDIMMs may only be installed in DIMM Slot 1 or 2 on a channel.
- 2 DPC QR Low Voltage RDIMMs are not supported.
- In order to install 3 QR LRDIMMs on the same channel, they must be operated with Rank Multiplication as RM = 2.
- RAS Modes Lockstep, Rank Sparing, and Mirroring are mutually exclusive in this BIOS. Only one operating mode may be selected, and it will be applied to the entire system.
- If a RAS Mode has been configured, and the memory population will not support it during boot, the system will fall back to Independent Channel Mode and log and display errors
- Rank Sparing Mode is only possible when all channels that are populated with memory meet the requirement of having at least 2 SR or DR DIMM installed, or at least one QR DIMM installed, on each populated channel.
- Lockstep or Mirroring Modes require that for any channel pair that is populated with memory, the memory population on both channels of the pair must be identically sized.

DIMM population rules require that DIMMs within a channel be populated starting with the BLUE DIMM slot or DIMM farthest from the processor in a “fill-farthest” approach. In addition, when populating a Quad-rank DIMM with a Single- or Dual-rank DIMM in the same channel, the Quad-rank DIMM must be populated farthest from the processor. Note that Quad-rand DIMMs and UDIMMs are not allowed in three slots populated configurations. Intel MRC will check for correct DIMM placement.

3.2.2.3 Publishing System Memory

- The BIOS displays the “Total Memory” of the system during POST if Display Logo is disabled in the BIOS setup. This is the total size of memory discovered by the BIOS during POST, and is the sum of the individual sizes of installed DDR3 DIMMs in the system.
- The BIOS displays the “Effective Memory” of the system in the BIOS setup. The term *Effective Memory* refers to the total size of all DDR3 DIMMs that are active (not disabled) and not used as redundant units.
- The BIOS provides the total memory of the system in the main page of the BIOS setup. This total is the same as the amount described by the first bullet above.

If Quite Boot is disabled, the BIOS displays the total system memory on the diagnostic screen at the end of POST. This total is the same as the amount described by the first bullet above.

3.2.2.4 RAS Features

The server board supports the following memory RAS modes:

- Independent Channel Mode
- Rank Sparing Mode
- Mirrored Channel Mode
- Lockstep Channel Mode

Regardless of RAS mode, the requirements for populating within a channel given in the section 3.2.2.2 must be met at all times. Note that support of RAS modes that require matching DIMM

population between channels (Mirrored and Lockstep) require that ECC DIMMs be populated. Independent Channel Mode is the only mode that supports non-ECC DIMMs in addition to ECC DIMMs.

For RAS modes that require matching populations, the same slot positions across channels must hold the same DIMM type with regards to size and organization. DIMM timings do not have to match but timings will be set to support all DIMMs populated (that is, DIMMs with slower timings will force faster DIMMs to the slower common timing modes).

3.2.2.4.1 Independent Channel Mode

Channels can be populated in any order in Independent Channel Mode. All four channels may be populated in any order and have no matching requirements. All channels must run at the same interface frequency but individual channels may run at different DIMM timings (RAS latency, CAS Latency, and so forth).

3.2.2.4.2 Rank Sparing Mode

In Rank Sparing Mode, one rank is a spare of the other ranks on the same channel. The spare rank is held in reserve and is not available as system memory. The spare rank must have identical or larger memory capacity than all the other ranks (sparing source ranks) on the same channel. After sparing, the sparing source rank will be lost.

3.2.2.4.3 Mirrored Channel Mode

In Mirrored Channel Mode, the memory contents are mirrored between Channel 0 and Channel 2 and also between Channel 1 and Channel 3. As a result of the mirroring, the total physical memory available to the system is half of what is populated. Mirrored Channel Mode requires that Channel 0 and Channel 2, and Channel 1 and Channel 3 must be populated identically with regards to size and organization. DIMM slot populations within a channel do not have to be identical but the same DIMM slot location across Channel 0 and Channel 2 and across Channel 1 and Channel 3 must be populated the same.

3.2.2.4.4 Lockstep Channel Mode

In Lockstep Channel Mode, each memory access is a 128-bit data access that spans Channel 0 and Channel 1, and Channel 2 and Channel 3. Lockstep Channel mode is the only RAS mode that allows SDDC for x8 devices. Lockstep Channel Mode requires that Channel 0 and Channel 1, and Channel 2 and Channel 3 must be populated identically with regards to size and organization. DIMM slot populations within a channel do not have to be identical but the same DIMM slot location across Channel 0 and Channel 1 and across Channel 2 and Channel 3 must be populated the same.

3.2.3 Processor Integrated I/O Module (IIO)

The processor's integrated I/O module provides features traditionally supported through chipset components. The integrated I/O module provides the following features:

3.2.3.1 PCI Express* Interfaces

The integrated I/O module incorporates the PCI Express* interface and supports up to 40 lanes of PCI Express*. Following are key attributes of the PCI Express* interface:

Intel® Server Board S2600IP and Intel® Workstation Board W2600CR supports PCI-e slots from two processors:

From first processor:

- Slot 1: PCIe Gen3 x16 connector
- Slot 2: PCIe Gen3 x8 connector.
- Slot 3: PCIe Gen3 x16 connector

From second processor:

- Slot 4: PCIe Gen3 x8 connector
- Slot 5: PCIe Gen3 x16 connector
- Slot 6: PCIe Gen3 x8 connector
- Slot 7: PCIe Gen3 x16 connector
- Slot 8: PCIe Gen2 x4 electrical with x8 physical connector.

Note: System will have video output on PCIe slots from first processor by default. If need add-in video card output on slots from second processor, please refer System Service guide to change Bios setup.

3.2.3.2 4.2.3.1.2 DMI2 Interface to the PCH

The platform requires an interface to the legacy Southbridge (PCH) which provides basic, legacy functions required for the server platform and operating systems. Since only one PCH is required and allowed for the system, any sockets which do not connect to PCH would use this port as a standard x4 PCI Express* 2.0 interface.

3.2.3.3 4.2.3.1.3 Integrated IOAPIC

Provides support for PCI Express* devices implementing legacy interrupt messages without interrupt sharing.

3.2.3.4 4.2.3.1.4 Non Transparent Bridge

PCI Express* non-transparent bridge (NTB) acts as a gateway that enables high performance, low overhead communication between two intelligent subsystems; the local and the remote subsystems. The NTB allows a local processor to independently configure and control the local subsystem, provides isolation of the local host memory domain from the remote host memory domain while enabling status and data exchange between the two domains.

3.2.3.5 4.2.3.1.5 Intel® QuickData Technology

Used for efficient, high bandwidth data movement between two locations in memory or from memory to I/O.

3.3 Intel® C600-A Chipset Functional overview

The Intel® C600-A Chipset in the Intel® Server Board S2600IP and Intel® Workstation Board W2600CR provide a connection point between various I/O components and Intel® Xeon Sandy Bridge-EP processors, which includes the following core platform functions:

- Digital Media Interface (DMI)
- PCI Express* Interface
- Serial ATA (SATA) Controller
- Serial Attached SCSI (SAS)/SATA Controller
- AHCI
- Rapid Storage Technology
- PCI Interface
- Low Pin Count (LPC) Interface
- Serial Peripheral Interface (SPI)
- Compatibility Modules (DMA Controller, Timer/Counters, Interrupt Controller)
- Advanced Programmable Interrupt Controller (APIC)
- Universal Serial Bus (USB) Controllers
- Gigabit Ethernet Controller
- RTC
- GPIO
- Enhanced Power Management
- Intel® Active Management Technology (Intel® AMT)
- Manageability
- System Management Bus (SMBus 2.0)
- Integrated NVSRAM controller
- Virtualization Technology for Directed I/O (Intel® VT-d)
- JTAG Boundary-Scan
- KVM/Serial Over LAN (SOL) Function

3.3.1 Digital Media Interface (DMI)

Digital Media Interface (DMI) is the chip-to-chip connection between the processor and The Intel® C600-A Chipset. This high-speed interface integrates advanced priority-based servicing allowing for concurrent traffic and true isochronous transfer capabilities. Base functionality is completely software-transparent, permitting current and legacy software to operate normally.

3.3.2 PCI Express* Interface

The Intel® C600-A Chipset provides up to 8 PCI Express* Root Ports, supporting the *PCI Express* Base Specification*, Revision 2.0. Each Root Port x1 lane supports up to 5 Gb/s bandwidth in each direction (10 Gb/s concurrent). PCI Express* Root Ports 1-4 or Ports 5-8 can independently be configured to support four x1s, two x2s, one x2 and two x1s, or one x4 port widths.

3.3.3 Serial ATA (SATA) Controller

The Intel® C600-A Chipset has two integrated SATA host controllers that support independent DMA operation on up to six ports and supports data transfer rates of up to 6.0 Gb/s (600 MB/s) on up to two ports (Port 0 and 1 Only) while all ports support rates up to 3.0 Gb/s (300 MB/s) and up to 1.5 Gb/s (150 MB/s). The SATA controller contains two modes of operation – a legacy mode using I/O space, and an AHCI mode using memory space. Software that uses legacy mode will not have AHCI capabilities.

The Intel® C600-A Chipset chipset supports the Serial ATA Specification, Revision 3.0. The Intel® C600-A Chipset also supports several optional sections of the Serial ATA II: Extensions to Serial ATA 1.0 Specification, Revision 1.0 (AHCI support is required for some elements).

3.3.4 Serial Attached SCSI (SAS)/SATA (SCU) Controller

The Intel® C600-A Chipset supports up to 8 SAS ports that are compliant with SAS 2.0 Specification and all ports support rates up to 3.0 Gb/s. All 8 ports are also independently configurable and compliant with SATA Gen2 and support data transfer rates of up to 3.0 Gb/s.

SAS/SATA controller is only available on specific Intel® C600-A Chipset SKUs with optional RAID C600 Upgrade key. Certain SKUs are also limited to support 4 of 8 SAS/SATA ports only. Please refer details below:

Note: SAS/SATA (SCU) port 0-3 is by default enabled while port 4-7 is disabled.

Table 7. Intel® RAID C600 Upgrade Key Options

Intel® RAID C600 Upgrade Key Options (Product Codes)	Key Color	Description
Default – No option key installed	N/A	4 Port SATA with Intel® ESRT RAID 0,1,10 and Intel® RSTe RAID 0,1,5,10
RKSATA4R5	Black	4 Port SATA with Intel® ESRT2 RAID 0,1, **5**, 10 and Intel® RSTe RAID 0,1,5,10
RKSATA8	Blue	8 Port SATA with Intel® ESRT2 RAID 0,1, 10 and Intel® RSTe RAID 0,1,5,10
RKSATA8R5	White	8 Port SATA with Intel® ESRT2 RAID 0,1, **5**, 10 and Intel® RSTe RAID 0,1,5,10
RKSAS4	Green	4 Port SAS with Intel® ESRT2 RAID 0,1, 10 and Intel® RSTe RAID 0,1,10
RKSAS4R5	Yellow	4 Port SAS with Intel® ESRT2 RAID 0,1, **5**, 10 and Intel® RSTe RAID 0,1,10
RKSAS8	Orange	8 Port SAS with Intel® ESRT2 RAID 0,1, 10 and Intel® RSTe RAID 0,1,10
RKSAS8R5	Purple	8 Port SAS with Intel® ESRT2 RAID 0,1, **5**, 10 and Intel® RSTe RAID 0,1,10

Additional information for the on-board RAID features and functionality can be found in the *Intel® RAID Software User's Guide* (Intel Document Number D29305-015).

3.3.5 AHCI

The Intel® C600-A Chipset provides hardware support for Advanced Host Controller Interface (AHCI), a standardized programming interface for SATA host controllers. Platforms supporting AHCI may take advantage of performance features. AHCI also provides usability enhancements such as Hot-Plug. AHCI requires appropriate software support (for example, an AHCI driver) and for some features, hardware support in the SATA device or additional platform hardware.

3.3.6 Rapid Storage Technology

The Intel® C600-A Chipset provides support for Intel® Rapid Storage Technology, providing both AHCI and integrated RAID functionality. The RAID capability provides high-performance RAID 0, 1, 5, and 10 functionality on the Intel® C600-A chipset. Matrix RAID support is provided to allow multiple RAID levels to be combined on a single set of hard drives, such as RAID 0 and

RAID 1 on two disks. Other RAID features include hot-spare support, SMART alerting, and RAID 0 auto replace.

3.3.7 PCI Interface

The Intel® C600-A chipset PCI interface provides a 33 MHz, Revision 2.3 implementation. The Intel® C600-A chipset integrates a PCI arbiter that supports up to four external PCI bus masters in addition to the internal Intel® C600-A chipset requests. This allows for combinations of up to four PCI down devices and PCI slots.

3.3.8 Low Pin Count (LPC) Interface

The Intel® C600-A chipset implements an LPC Interface as described in the LPC 1.1 Specification. The Low Pin Count (LPC) bridge function of the Intel® C600-A resides in PCI Device 31: Function 0. In addition to the LPC bridge interface function, D31:F0 contains other functional units including DMA, interrupt controllers, timers, power management, system management, GPIO, and RTC.

3.3.9 Serial Peripheral Interface (SPI)

The Intel® C600-A chipset implements an SPI Interface as an alternative interface for the BIOS flash device. The SPI flash is required to support Gigabit Ethernet and Intel® Active Management Technology. The Intel® C600-A chipset supports up to two SPI flash devices with speeds up to 50 MHz.

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

The DMA controller incorporates the logic of two 82C37 DMA controllers, with seven independently programmable channels. The Intel® C600-A chipset supports LPC DMA through the Intel® C600-A chipset's DMA controller.

The timer/counter block contains three counters that are equivalent in function to those found in one 82C54 programmable interval timer. These three counters are combined to provide the system timer function, and speaker tone.

The Intel® C600-A chipset provides an ISA-Compatible Programmable Interrupt Controller (PIC) that incorporates the functionality of two 82C59 interrupt controllers. In addition, the Intel® C600-A chipset supports a serial interrupt scheme.

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

3.3.11 Advanced Programmable Interrupt Controller (APIC)

In addition to the standard ISA compatible Programmable Interrupt controller (PIC) described in the previous section, the Intel® C600-A incorporates the Advanced Programmable Interrupt Controller (APIC).

3.3.12 Universal Serial Bus (USB) Controllers

The Intel® C600-A chipset has up to two Enhanced Host Controller Interface (EHCI) host controllers that support USB high-speed signaling. High-speed USB 2.0 allows data transfers up to 480 Mb/s which is 40 times faster than full-speed USB. The Intel® C600-A chipset supports

up to fourteen USB 2.0 ports. All fourteen ports are high-speed, full-speed, and low-speed capable.

3.3.13 Gigabit Ethernet Controller

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

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

3.3.14 RTC

The Intel® C600-A chipset contains a real-time clock with 256 bytes of battery-backed RAM. The real-time clock performs two key functions: keeping track of the time of day and storing system data. The RTC operates on a 32.768 KHz crystal and a 3 V battery.

3.3.15 GPIO

Various general purpose inputs and outputs are provided for custom system design. The number of inputs and outputs varies depending on the Intel® C600-A chipset configuration.

3.3.16 Enhanced Power Management

The Intel® C600-A chipset's power management functions include enhanced clock control and various low-power (suspend) states (for example, Suspend-to-RAM and Suspend-to-Disk). A hardware-based thermal management circuit permits software-independent entrance to low-power states. The Intel® C600-A chipset contains full support for the Advanced Configuration and Power Interface (ACPI) Specification, Revision 4.0a.

3.3.17 Manageability

In addition to Intel AMT the Intel® C600-A chipset integrates several functions designed to manage the system and lower the total cost of ownership (TCO) of the system. These system management functions are designed to report errors, diagnose the system, and recover from system lockups without the aid of an external microcontroller.

3.3.18 System Management Bus (SMBus 2.0)

The Intel® C600-A chipset contains a SMBus Host interface that allows the processor to communicate with SMBus slaves. This interface is compatible with most I2C devices. Special I2C commands are implemented.

The Intel® C600-A chipset's SMBus host controller provides a mechanism for the processor to initiate communications with SMBus peripherals (slaves). Also, the Intel® C600-A chipset

supports slave functionality, including the Host Notify protocol. Hence, the host controller supports eight command protocols of the SMBus interface (see System Management Bus (SMBus) Specification, Version 2.0): Quick Command, Send Byte, Receive Byte, Write Byte/Word, Read Byte/Word, Process Call, Block Read/Write, and Host Notify.

The Intel® C600-A chipset's SMBus also implements hardware-based Packet Error Checking for data robustness and the Address Resolution Protocol (ARP) to dynamically provide address to all SMBus devices.

3.3.19 Integrated NVSRAM controller

The Intel® C600-A chipset has an integrated NVSRAM controller that supports up to 32KB external device. The host processor can read and write data to the NVSRAM component.

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

The Intel® C600-A chipset provides hardware support for implementation of Intel® Virtualization Technology with Directed I/O (Intel® VT-d). Intel VT-d consists of technology components that support the virtualization of platforms based on Intel® Architecture Processors. Intel VT-d Technology enables multiple operating systems and applications to run in independent partitions. A partition behaves like a virtual machine (VM) and provides isolation and protection across partitions. Each partition is allocated its own subset of host physical memory.

3.3.21 JTAG Boundary-Scan

The Intel® C600-A chipset adds the industry standard JTAG interface and enables Boundary-Scan in place of the XOR chains used in previous generations of chipsets. Boundary-Scan can be used to ensure device connectivity during the board manufacturing process. The JTAG interface allows system manufacturers to improve efficiency by using industry available tools to test the Intel® C600-A chipset on an assembled board. Since JTAG is a serial interface, it eliminates the need to create probe points for every pin in an XOR chain. This eases pin breakout and trace routing and simplifies the interface between the system and a bed-of-nails tester.

3.3.22 KVM/Serial Over Lan (SOL) Function

These functions support redirection of keyboard, mouse, and text screen to a terminal window on a remote console. The keyboard, mouse, and text redirection enables the control of the client machine through the network. Text, mouse, and keyboard redirection allows the remote machine to control and configure the client by entering BIOS setup. The KVM/SOL function emulates a standard PCI serial port and redirects the data from the serial port to the management console using LAN. KVM has additional requirements of internal graphics and SOL may be used when KVM is not supported.

3.3.23 On-board SAS/SATA Support and Options

The Intel® C600 chipset provides storage support by two integrated controllers: AHCI and SCU. By default the server board will support up to 10 SATA ports: Two white 6Gb/sec SATA ports from the AHCI controller labeled as "SATA_0" and "SATA_1" and two MINISAS 3Gb/sec SATA/SAS ports routed from the SCU controller
labeled as "SCU0 (PORT0-3) and "SCU1(PORT4-7).

The SCU Port can be configured with the two embedded software RAID options:

- Intel® Embedded Server RAID Technology 2 (ESRT2) based on LSI* MegaRAID SW

RAID technology supporting RAID levels 0,1, and 10.

- Intel® Rapid Storage Technology (RSTe) supporting RAID levels 0, 1, 5, and 10.

3.3.23.1 Intel® Embedded Server RAID Technology 2 (ESRT2)

Features of the embedded software RAID option Intel® Embedded Server RAID Technology 2 (ESRT2) include the following:

- Based on LSI* MegaRAID Software Stack
- Software RAID with system providing memory and CPU utilization
- Supported RAID Levels – 0,1,5,10
  - 4 and 8 Port SATA RAID 5 support provided with appropriate Intel® RAID C600 Upgrade Key
  - 4 and 8 Port SAS RAID 5 support provided with appropriate Intel® RAID C600 Upgrade Key
- Maximum drive support = 8
- Open Source Compliance = Binary Driver (includes Partial Source files) or Open Source using MDRAID layer in Linux.
- OS Support = Windows 7*, Windows 2008*, Windows 2003*, RHEL*, SLES, other Linux* variants using partial source builds.
- Utilities = Windows* GUI and CLI, Linux GUI and CLI, DOS CLI, and EFI CLI

3.3.23.2 Intel® Rapid Storage Technology (RSTe)

Features of the embedded software RAID option Intel® Rapid Storage Technology (RSTe) include the following:

- Software RAID with system providing memory and CPU utilization
- Supported RAID Levels – 0,1,5,10
  - 4 Port SATA RAID 5 available standard (no option key required)
  - 8 Port SATA RAID 5 support provided with appropriate Intel® RAID C600 Upgrade Key
  - No SAS RAID 5 support
- Maximum drive support = 32 (in arrays with 8 port SAS), 16 (in arrays with 4 port SAS), 128 (JBOD)
- Open Source Compliance = Yes (uses MDRAID)
- OS Support = Windows 7*, Windows 2008*, Windows 2003*, RHEL* 6.2 and later, SLES* 11 w/SP2 and later, VMWare* 5.x.
- Utilities = Windows* GUI and CLI, Linux CLI, DOS CLI, and EFI CLI
- Uses Matrix Storage Manager for Windows*
- MDRAID supported in Linux* (does not require a driver)

Note: No boot drive support to targets attached through SAS expander card

3.4 PCI Subsystem

The primary I/O buses for the Intel® Server Board S2600IP and Intel® Workstation Board W2600CR are PCI Express* Gen3 with six independent PCI bus segments. The following tables list the characteristics of the PCI bus segments.

Table 8. Intel® Server Board S2600IP/Workstation Board W2600CR PCI Bus Segment Characteristics

Voltage	Width	Speed	Type	PCI I/O Card Slots
3.3 V	x16	32 GB/S	PCI Express* Gen3	X16 PCI Express* Gen3 throughput to Slot1 (x16 mechanically)
3.3 V	X8 or none (with mux)	16 GB/S or none	PCI Express* Gen3	x8 PCI Express* Gen3 throughput to Slot 2 (x8 mechanically)
3.3 V	x16 or x8(with mux)	32 GB/S or 16 GB/S	PCI Express* Gen3	x16 PCI Express* Gen3 throughput to Slot 3 (x16 mechanically)
3.3 V	X8 or none (with mux)	16 GB/S or none	PCI Express* Gen3	x8 PCI Express* Gen3 throughput to Slot 4 (x8 mechanically, Non-Persistent)
3.3 V	x16 or x8(with mux)	32 GB/S or 16 GB/S	PCI Express* Gen3	X16 PCI Express* Gen3 throughput to Slot 5 (x16 mechanically, Non-Persistent)
3.3 V	X8 or none (with mux)	16 GB/S or none	PCI Express* Gen3	x8 PCI Express* Gen3 throughput to Slot 6 (x8 mechanically, Non-Persistent)
3.3 V	x16 or x8(with mux)	32 GB/S or 16 GB/S	PCI Express* Gen3	X16 PCI Express* Gen3 throughput to Slot 7 (x16 mechanically, Non-Persistent)
3.3 V	x8	4 GB/S	PCI Express* Gen3	x8 PCI Express* Gen3 throughput to Slot 8 (x8 mechanically, Non-Persistent, Open Ended)

3.5 Network Interface Controller

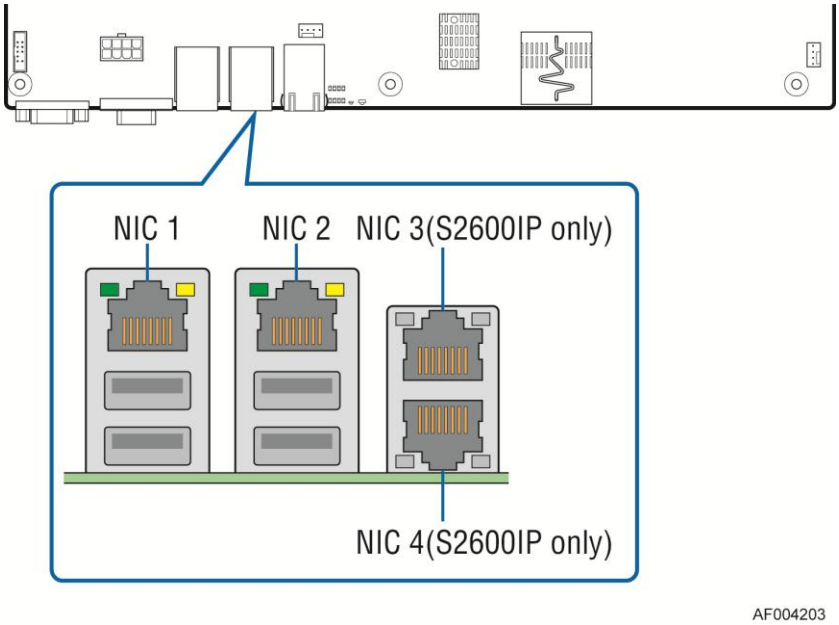
The Intel® Server Board S2600IP and Workstation Board S2600CR has a Intel® Ethernet Controller I350 GbE Controller. The controller supports PCI Express* PCIe v2.0 (5GT/s and 2.5GT/s). The controller enables four-port or two-port 1000BASE-T implementations using integrated PHY's. The controller supports VMDq, SR-IOV, EEE, and DMA Coalescing.

3.5.1 Network Interface

Network connectivity is provided by means of an onboard Intel® Ethernet Controller 1350-AM4 providing up to four 10/100/1000 Mb Ethernet ports.

On the Intel® Server Board S2600IP, four external 10/100/1000 Mb RJ45 Ethernet ports are provided. On the Intel® Workstation Board W2600CR, two external 10/100/1000 Mb RJ45 Ethernet ports are provided. Each Ethernet port drives two LEDs located on each network interface connector. The LED at the right of the connector is the link/activity LED and indicates

network connection when on, and transmit/receive activity when blinking. The LED at the left of the connector indicates link speed as defined in the following table.



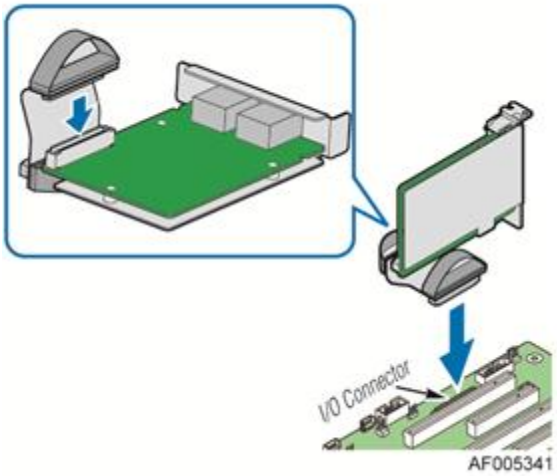
LED Color	LED State	NIC State
Green/Amber (Right)	Off	10 Mbps
	Amber	100 Mbps
	Green	1000 Mbps
Green (Left)	On	Active Connection
	Blinking	Transmit/Receive activity

Figure 20. External RJ45 NIC Port LED Definition

3.6 I/O Module Support (not avaiable for Intel® Server Board S2600IP4L and Intel® Workstation Board W2600CR2L)

To broaden the standard on-board feature set, the server board supports the option of adding a single I/O module providing external ports for a variety of networking interfaces. The I/O module attaches to a high density 80-pin connector on the server board labeled “IO_Module”.

Supported I/O modules include:



Product Code and iPN	Description
AXX10GBNIAIOM MM# 917905	Dual SFP+ port 10GbE IO Module based on Intel® 82599 10GbE Ethernet Controller
AXX10GBTWLIOM MM# 917907	Dual RJ45 Port, 10GBASE-T IO Module, based on Intel® I350 Ethernet chipset
AXX1FDRIBIOM MM# 918607	Single Port, FDR speed Infiniband* module, with QSFP connector.
AXX4P1GBPWLIOM MM# 917911	Quad Port 1GbE 1o Module based on Intel® Ethernet Controller I350
AXXIOMKIT MM# 920852	I/O Module Cable and Brackets

Figure 21. Supported I/O Module Options

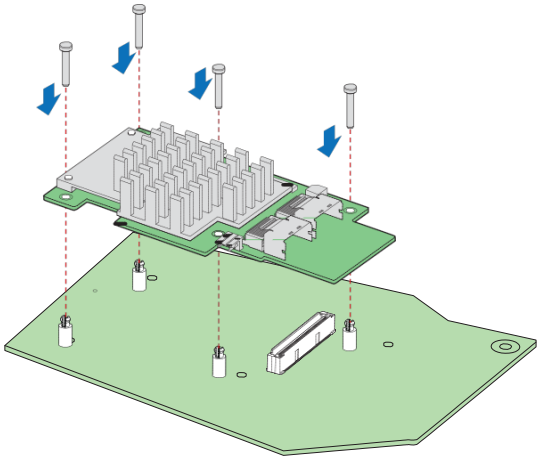
Notes:
I/O Module cable and Brackets accessory is necessary to support I/O module on Intel® Server Board S2600IP.

3.7 SAS ROC Module Support

The system provides support for Intel® Integrated RAID mezzanine modules that utilize a high density 80-pin connector (labeled “SAS_MOD”) on the server board.

Features of this option include:

- Does not utilize a PCIe slot
- SKU options to support full or entry level hardware RAID
- 4 or 8 port and SAS/SATA or SATA –only ROC options



- SKU options to support 512MB or 1GB embedded memory
- Intel designed flash + optional support for super-cap backup (Maintenance Free Back Up) or improved Lithium Polymer battery

Table 9. Supported Intel® Integrated RAID Modules

External Name	Description	Product Code
Intel® Integrated RAID Module RMS25CB080	8 Port SAS-2.1, Full HW RAID, 1GB, IOM Slot RAID Levels 0,1,10, 5, 50, 6, 60	RMS25CB080
Intel® Integrated RAID Module RMS25CB040	4 Port SAS-2.1, Full HW RAID, 1GB, IOM Slot RAID Levels 0,1,10, 5, 50, 6, 60	RMS25CB040
Intel® Integrated RAID Module RMT3CB080	8 Port SATA-3, Full HW RAID, 512MB, IOM Slot RAID Levels 0,1,10, 5, 50, 6, 60	RMT3CB080
Intel® Integrated RAID Module RMS25KB080	8 Port SAS-2.1, Entry-level HW RAID, IOM Slot RAID Levels 0,1,1E	RMS25KB080
Intel® Integrated RAID Module RMS25KB040	4 Port SAS-2.1, Entry-level HW RAID, IOM Slot RAID Levels 0,1,1E	RMS25KB040

For additional product information, please refer the following Intel® document:
Intel® Integrated RAID Module RMS25PB080, RMS25PB040, RMS25CB080, and RMS25CB040 Hardware User's Guide – Intel Order Number G37519-002.

3.8 HD Audio Support (Intel® Workstation Board W2600CR Only)

The Intel® Workstation Board W2600CR support 7.1 HD Audio through the High Definition Audio Codec Realtek* ALC889. The ALC889 provides ten DAC channels that simultaneously support 7.1 sound playback, plus two channels of independent stereo sound output (multiple streaming) through the front panel stereo outputs. Also supports two channels of S/PDIF In/Out (W2600CR only supports 1 S/PDIF Out port) and two channels of Microphone In (Front/Rear). The ALC889 is driven by the Intel HD Audio Interface (Azalia) from Intel® C600-A chipset.

Table 10: Standard Speaker Channels

Channel name	Identifier	1.0 Mono	2.0 Stereo	5.1 Surround	7.1 Surround
Front Left	SPEAKER_FRONT_LEFT	No	Yes	Yes	Yes
Front Right	SPEAKER_FRONT_RIGHT	No	Yes	Yes	Yes
Front Center	SPEAKER_FRONT_CENTER	Yes	No	Yes	Yes
Low Frequency (Subwoofer)	SPEAKER_LOW_FREQUENCY	No	No	Yes	Yes
Back Left	SPEAKER_BACK_LEFT	No	No	Yes	Yes
Back Right	SPEAKER_BACK_RIGHT	No	No	Yes	Yes
Side Left	SPEAKER_SIDE_LEFT	No	No	No	Yes
Side Right	SPEAKER_SIDE_RIGHT	No	No	No	Yes

3.9 USB3.0 Support (Intel® Workstation Board W2600CR Only)

The Intel® Workstation Board W2600CR supports two USB3.0 SuperSpeed* ports, which is required as a standard Workstation feature. The TI 2 port USB3.0 discrete host controller TUSB7320 is used to meet this requirement. The TUSB7320 USB3.0 host controller complies with *Universal Serial Bus 3.0 Specification* and Intel's eXtensible Host Controller Interface (xHCI).

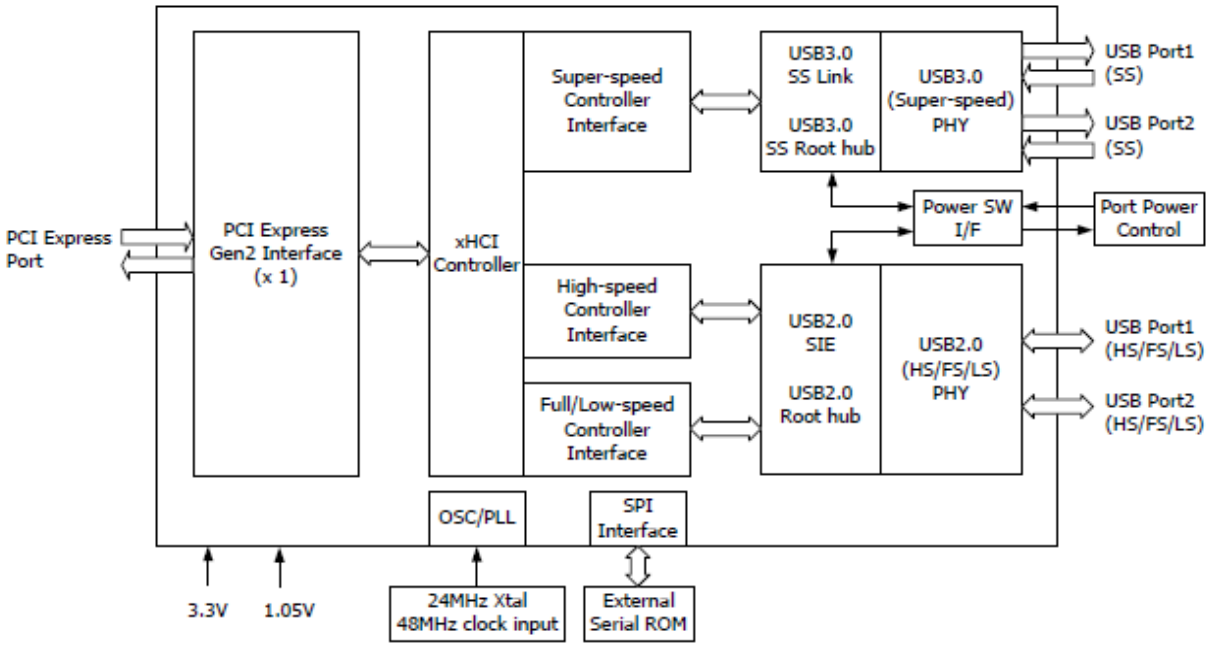


Figure 22.USB3.0 Discrete Host Controller Block Diagram

3.10 IEEE1394b Support (Intel® Workstation Board W2600CR Only)

Intel® Workstation Board W2600CR offers one front panel IEEE 1394b port from a discrete controller (Texas Instruments XIO2221).The XIO2221 uses a PCIe x1 Gen 1 upstream interface from Intel® C600-A chipset. When connected to 1394b compliant devices, the XIO2221 can transfer data at speeds of up to 800 Mbps. The Intel® Workstation Board W2600CR includes an internal 1394b connector that allows for a front panel 1394b cable attach.

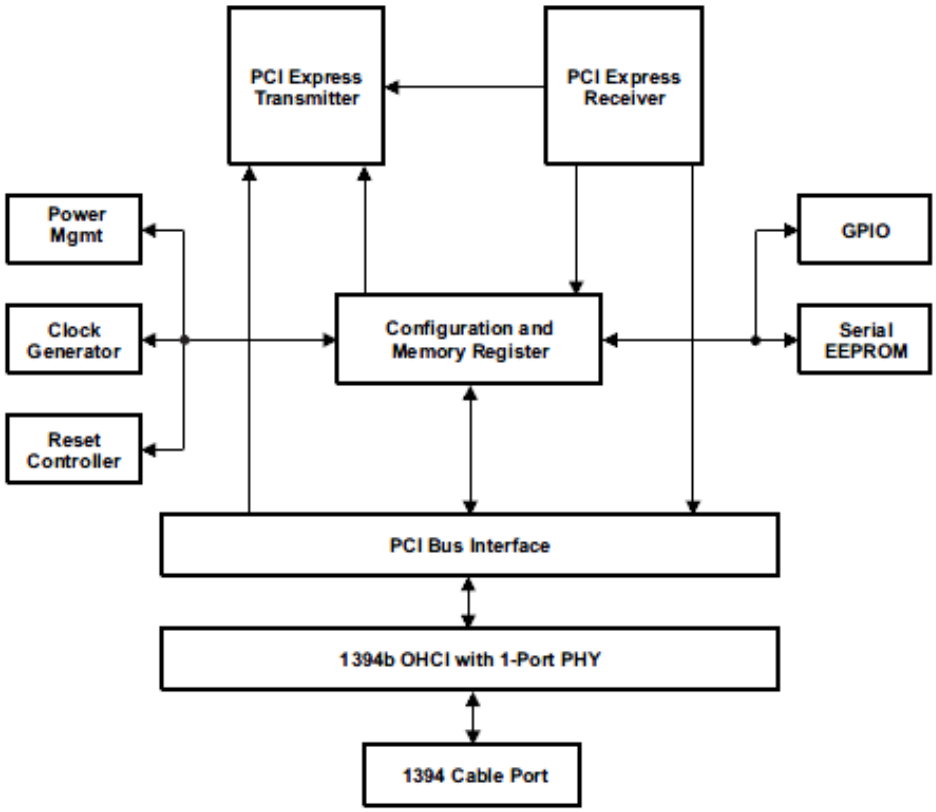


Figure 23.IEEE 1394b Discrete Host Controller Block Diagram

4. Platform Management Overview

4.1 Server Management Function Architecture

4.1.1 Feature Support

4.1.1.1 IPMI 2.0 Features

The IPMI 2.0 features are as follows:

1. Baseboard management controller (BMC)
2. IPMI Watchdog timer
3. Messaging support, including command bridging and user/session support
4. Chassis device functionality, including power/reset control and BIOS boot flags support
5. Event receiver device: The BMC receives and processes events from other platform subsystems.
6. Field Replaceable Unit (FRU) inventory device functionality: The BMC supports access to system FRU devices using IPMI FRU commands.
7. System Event Log (SEL) device functionality: The BMC supports and provides access to a SEL.
8. Sensor Data Record (SDR) repository device functionality: The BMC supports storage and access of system SDRs.
9. Sensor device and sensor scanning/monitoring: The BMC provides IPMI management of sensors. It polls sensors to monitor and report system health.
10. IPMI interfaces
11. Host interfaces include system management software (SMS) with receive message queue support, and server management mode (SMM)
12. IPMB interface
13. LAN interface that supports the IPMI-over-LAN protocol Remote Management Control Protocol (RMCP, RMCP+)
14. Serial-over-LAN (SOL)
15. ACPI state synchronization: The BMC tracks ACPI state changes that are provided by the BIOS.
16. BMC self test: The BMC performs initialization and run-time self-tests and makes results available to external entities.

See also the *Intelligent Platform Management Interface Specification Second Generation,* Version 2.0.

4.1.1.2 Non IPMI features

The BMC supports the following non-IPMI features. This list does not preclude support for future enhancements or additions.

- In-circuit BMC firmware update
- Fault resilient booting (FRB): FRB2 is supported by the watchdog timer functionality.

- Chassis intrusion detection (dependent on platform support)
- Basic fan control using Control version 2 SDRs
- Fan redundancy monitoring and support
- Power supply redundancy monitoring and support
- Hot-swap fan support
- Acoustic management: Support for multiple fan profiles
- Signal testing support: The BMC provides test commands for setting and getting platform signal states.
- The BMC generates diagnostic beep codes for fault conditions.
- System GUID storage and retrieval
- Front panel management: The BMC controls the system status LED and chassis ID LED. It supports secure lockout of certain front panel functionality and monitors button presses. The chassis ID LED is turned on using a front panel button or a command.
- Power state retention
- Power fault analysis
- Intel® Light-Guided Diagnostics
- Power unit management: Support for power unit sensor. The BMC handles power-good dropout conditions.
- DIMM temperature monitoring: New sensors and improved acoustic management using closed-loop fan control algorithm taking into account DIMM temperature readings.
- Address Resolution Protocol (ARP): The BMC sends and responds to ARPs (supported on embedded NICs).
- Dynamic Host Configuration Protocol (DHCP): The BMC performs DHCP (supported on embedded NICs).
- Platform environment control interface (PECI) thermal management support
- E-mail alerting
- Embedded web server
- Integrated KVM.
- Integrated Remote Media Redirection
- Lightweight Directory Access Protocol (LDAP) support
- Intel® Intelligent Power Node Manager support

4.1.1.3 New Manageability Features

Intel® S1400/S1600/S2400/S2600 Server Platforms offer a number of changes and additions to the manageability features that are supported on the previous generation of servers. The following is a list of the more significant changes that are common to this generation Integrated BMC based Intel® Server boards:

- Sensor and SEL logging additions/enhancements (for example, additional thermal monitoring capability)
- SEL Severity Tracking and the Extended SEL

- Embedded platform debug feature which allows capture of detailed data for later analysis.
- Provisioning and inventory enhancements:
  - Inventory data/system information export (partial SMBIOS table)
- Enhancements to fan speed control.
- DCMI 1.1 compliance (product-specific).
- Support for embedded web server UI in *Basic Manageability* feature set.
- Enhancements to embedded web server
  - Human-readable SEL
  - Additional system configurability
  - Additional system monitoring capability
  - Enhanced on-line help
- Enhancements to KVM redirection
  - Support for higher resolution
- Support for EU Lot6 compliance
- Management support for PMBus rev1.2 compliant power supplies
- BMC Data Repository (Managed Data Region Feature)
- Local Control Display Panel
- System Airflow Monitoring
- Exit Air Temperature Monitoring
- Ethernet Controller Thermal Monitoring
- Global Aggregate Temperature Margin Sensor
- Memory Thermal Management
- Power Supply Fan Sensors
- Energy Star Server Support
- Smart Ride Through (SmaRT)/ Closed Loop System Throttling (CLST)
- Power Supply Cold Redundancy
- Power Supply FW Update
- Power Supply Compatibility Check
- BMC FW reliability enhancements:
  - Redundant BMC boot blocks to avoid possibility of a corrupted boot block resulting in a scenario that prevents a user from updating the BMC.
  - BMC System Management Health Monitoring

4.1.2 Basic and Advanced Features

The bellowing table lists basic and advanced feature support. Individual features may vary by platform. See the appropriate Platform Specific EPS addendum for more information.

Table 11. Basic and Advanced Features

Feature	Basic	Advanced
IPMI 2.0 Feature Support	X	X
In-circuit BMC Firmware Update	X	X
FRB 2	X	X
Chassis Intrusion Detection	X	X
Fan Redundancy Monitoring	X	X
Hot-Swap Fan Support	X	X
Acoustic Management	X	X
Diagnostic Beep Code Support	X	X
Power State Retention	X	X
ARP/DHCP Support	X	X
PECI Thermal Management Support	X	X
E-mail Alerting	X	X
Embedded Web Server	X	X
SSH Support	X	X
Integrated KVM		X
Integrated Remote Media Redirection		X
Lightweight Directory Access Protocol (LDAP)	X	X
Intel® Intelligent Power Node Manager Support	X	X
SMASH CLP	X	X

4.1.3 Integrated BMC Hardware: Emulex* Pilot III

4.1.3.1 Emulex* Pilot III Baseboard Management Controller Functionality

The Integrated BMC is provided by an embedded ARM9 controller and associated peripheral functionality that is required for IPMI-based server management. Firmware usage of these hardware features is platform dependent.

The following is a summary of the Integrated BMC management hardware features that comprise the BMC:

- 400MHz 32-bit ARM9 processor with memory management unit (MMU)
- Two independent10/100/1000 Ethernet Controllers with Reduced Media Independent Interface (RMII)/ Reduced Gigabit Media Independent Interface (RGMII) support
- DDR2/3 16-bit interface with up to 800 MHz operation
- 16 10-bit ADCs
- Sixteen fan tachometers
- Eight Pulse Width Modulators (PWM)
- Chassis intrusion logic
- JTAG Master
- Eight I^2C interfaces with master-slave and SMBus timeout support. All interfaces are SMBus 2.0 compliant.
- Parallel general-purpose I/O Ports (16 direct, 32 shared)
- Serial general-purpose I/O Ports (80 in and 80 out)
- Three UARTs
- Platform Environmental Control Interface (PECI)

- Six general-purpose timers
- Interrupt controller
- Multiple Serial Peripheral Interface (SPI) flash interfaces
- NAND/Memory interface
- Sixteen mailbox registers for communication between the BMC and host
- LPC ROM interface
- BMC watchdog timer capability
- SD/MMC card controller with DMA support
- LED support with programmable blink rate controls on GPIOs
- Port 80h snooping capability
- Secondary Service Processor (SSP), which provides the HW capability of offloading time critical processing tasks from the main ARM core.

Emulex* Pilot III contains an integrated SIO, KVMS subsystem and graphics controller with the following features:

4.1.3.1.1 Super I/O (SIO)

The BMC integrates a super I/O module with the following features:

- Keyboard Style/BT interface for BMC support
- Two Fully Functional Serial Ports, compatible with the 16C550
- Serial IRQ Support
- Up to 16 Shared GPIO available for host processor
- Programmable Wake-up Event Support
- Plug and Play Register Set
- Power Supply Control

4.1.3.1.2 Graphics Controller

The graphics controller provides the following features:

- Integrated Graphics Core with 2D Hardware accelerator
- High speed Integrated 24-bit RAMDAC
  DDR-2/3 memory interface with 16Mbytes of memory allocated and reported for graphics memory.

4.1.3.1.3 Remote Keyboard, Video, Mouse, and Storage (KVMS)

The Integrated BMC contains a remote KVMS subsystem with the following features:

- USB 2.0 interface for Keyboard, Mouse and Remote storage such as CD/DVD ROM and floppy
- USB 1.1/USB 2.0 interface for PS2 to USB bridging, remote Keyboard and Mouse
- Hardware Based Video Compression and Redirection Logic
- Supports both text and Graphics redirection
- Hardware assisted Video redirection using the Frame Processing Engine
- Direct interface to the Integrated Graphics Controller registers and Frame buffer
- Hardware-based encryption engine

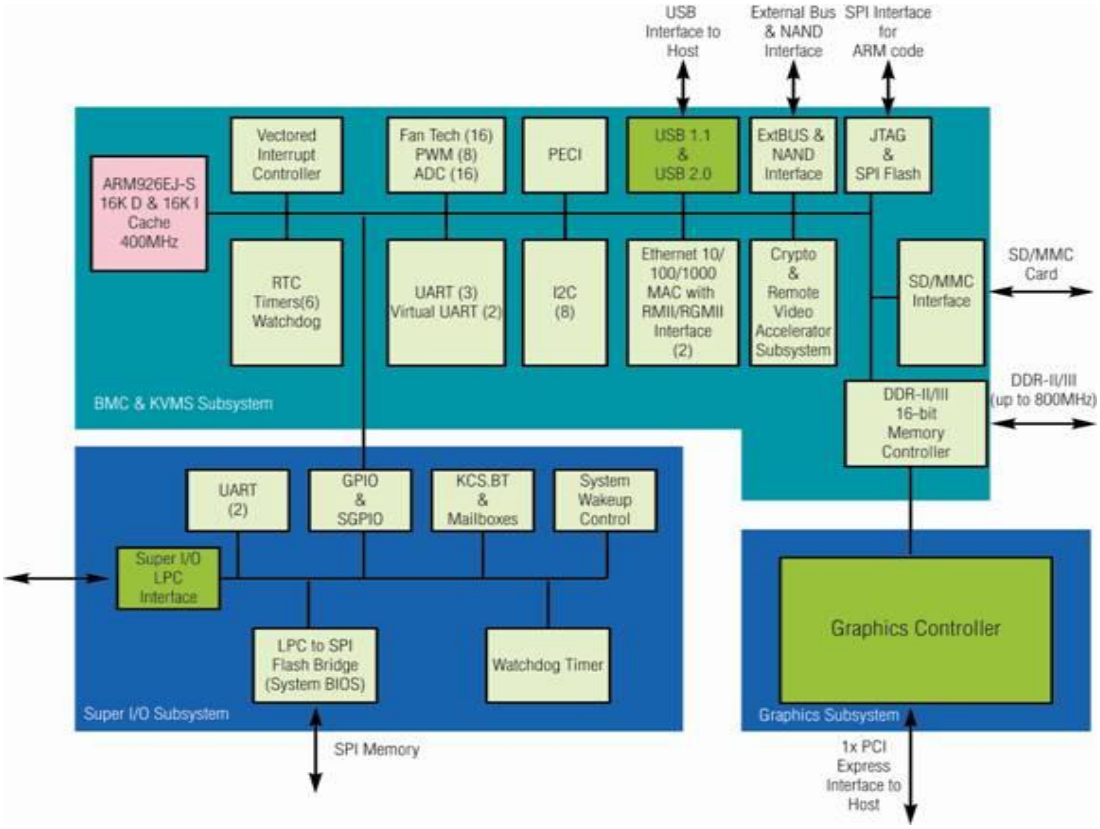


Figure 24. Integrated BMC Hardware

4.2 Server Management Functional Specifications

4.2.1 BMC Internal Timestamp Clock

The BMC maintains an internal timestamp clock that is used by various BMC subsystems, for example, time stamping SEL entries. As part of BMC initialization after AC power is applied or the BMC is reset, the BMC initializes this internal clock to the value retrieved from the SSB component's RTC from a SMBus slave read operation. This is the system RTC and is on the battery power well so it maintains the current time even when there is no AC supplied to the system.

4.2.1.1 System Clock Synchronization

The BIOS must send the *Set SEL Time* command with the current system time to the BMC during system Power-on Self Test (POST). Synchronization during very early POST is preferred, so that any SEL entries recorded during system boot can be accurately time stamped. Additionally, during sleep state transitions other than S0 the BIOS will synchronize the time.

If the time is modified through an OS interface, then the BMC's time is not synchronized until the next system reboot.

4.2.2 System Event Log (SEL)

The BMC implements the system event log as specified in the *Intelligent Platform Management Interface Specification, Version 2.0.* The SEL is accessible regardless of the system power state through the BMC's in-band and out-of-band interfaces.

The BMC allocates 95231 bytes (approximately 93 KB) of non-volatile storage space to store system events. The SEL timestamps may not be in order. Up to 3,639 SEL records can be stored at a time. Any command that results in an overflow of the SEL beyond the allocated space is rejected with an “Out of Space” IPMI completion code (C4h).

4.2.3 Sensor Data Record (SDR) Repository

The BMC implements the sensor data record (SDR) repository as specified in the *Intelligent Platform Management Interface Specification, Version 2.0.* The SDR is accessible through the BMC’s in-band and out-of-band interfaces regardless of the system power state The BMC allocates 65,519 bytes of non-volatile storage space for the SDR.

4.2.4 Field Replaceable Unit (FRU) Inventory Device

The BMC implements the interface for logical FRU inventory devices as specified in the *Intelligent Platform Management Interface Specification, Version 2.0.* This functionality provides commands used for accessing and managing the FRU inventory information. These commands can be delivered through all interfaces.

The BMC provides FRU device command access to its own FRU device and to the FRU devices throughout the server. The FRU device ID mapping is defined in the Platform Specific Information. The BMC controls the mapping of the FRU device ID to the physical device.

4.2.5 BMC Beep Codes

The BMC may generate beep codes upon detection of failure conditions. Beep codes are sounded each time the problem is discovered (for example, on each power-up attempt), but are not sounded continuously. Common supported codes are listed in below Table

Additional platform-specific beep codes can be found in the appropriate Platform Specific Information. Each digit in the code is represented by a sequence of beeps whose count is equal to the digit.

Table 12. BMC Beep Codes

Code	Reason for Beep	Associated Sensors
1-5-2-1	No CPUs installed or first CPU socket is empty.	CPU Missing Sensor
1-5-2-4	MSID Mismatch.	MSID Mismatch Sensor.
1-5-4-2	Power fault: DC power is unexpectedly lost (power good dropout).	Power unit – power unit failure offset.
1-5-4-4	Power control fault (power good assertion timeout).	Power unit – soft power control failure offset.
1-5-1-2	VR Watchdog Timer sensor assertion	VR Watchdog Timer

Code	Reason for Beep	Associated Sensors
1-5-1-4	The system does not power on or unexpectedly powers off and a power supply unit (PSU) is present that is an incompatible model with one or more other PSUs in the system	PS Status

4.2.6 Diagnostic Interrupt (NMI) Button

The BMC generates an NMI pulse under certain conditions. The BMC-generated NMI pulse duration is at least 30 ms. Once an NMI has been generated by the BMC, the BMC does not generate another NMI until the system has been reset or powered down.

The following actions cause the BMC to generate an NMI pulse:

1. Receiving a *Chassis Control* command to pulse the diagnostic interrupt. This command does not cause an event to be logged in the SEL.
2. Watchdog timer pre-timeout expiration with NMI/diagnostic interrupt pre-timeout action enabled.

   The following table shows the behavior regarding NMI signal generation and event logging by the BMC.

Table 13. NMI Signal Generation and Event Logging

Causal Event	NMI	
	Signal Generation	Front Panel Diag Interrupt Sensor Event Logging Support
Chassis Control command (pulse diagnostic interrupt)	X	–
Front panel diagnostic interrupt button pressed	X	X
Watchdog Timer pre-timeout expiration with NMI/diagnostic interrupt action	X	X

4.2.7 BMC Watchdog

The BMC FW is increasingly called upon to perform system functions that are time-critical in that failure to provide these functions in a timely manner can result in system or component damage. Intel® S1400/S1600/S2400/S2600 Server Platforms introduce a BMC watchdog feature to provide a safe-guard against this scenario by providing an automatic recovery mechanism. It also can provide automatic recovery of functionality that has failed due to a fatal FW defect triggered by a rare sequence of events or a BMC hang due to some type of HW glitch (for example, power).

This feature is comprised of a set of capabilities whose purpose is to detect misbehaving subsections of BMC firmware, the BMC CPU itself, or HW subsystems of the BMC component, and to take appropriate action to restore proper operation. The action taken is dependent on the nature of the detected failure and may result in a restart of the BMC CPU, one or more BMC HW subsystems, or a restart of malfunctioning FW subsystems.

The BMC watchdog feature will only allow up to three resets of the BMC CPU (such as HW reset) or entire FW stack (such as a SW reset) before giving up and remaining in the uBOOT

code. This count is cleared upon cycling of power to the BMC or upon continuous operation of the BMC without a watchdog-generated reset occurring for a period of > 30 minutes. The BMC FW logs a SEL event indicating that a watchdog-generated BMC reset (either soft or hard reset) has occurred. This event may be logged after the actual reset has occurred. Refer sensor section for details for the related sensor definition. The BMC will also indicate a degraded system status on the Front Panel Status LED after an BMC HW reset or FW stack reset. This state (which follows the state of the associated sensor) will be cleared upon system reset or (AC or DC) power cycle.

Note: A reset of the BMC may result in the following system degradations that will require a system reset or power cycle to correct:

1. Timeout value for the rotation period can be set using this parameter; potentially incorrect ACPI Power State reported by the BMC.
2. Reversion of temporary test modes for the BMC (for example, as set through Set SM Signal command) back to normal operational modes.
3. FP status LED and DIMM fault LEDs may not reflect BIOS detected errors.

4.3 Sensor Monitoring

4.3.1 Overview

The BMC monitors system hardware and reports system health. The information gathered from physical sensors is translated into IPMI sensors as part of the “IPMI Sensor Model”. The BMC also reports various system state changes by maintaining virtual sensors that are not specifically tied to physical hardware. This section describes the BMC sensors as well as describing how specific sensor types are modeled. Unless otherwise specified, the term “sensor” refers to the IPMI sensor-model definition of a sensor.

4.3.2 Core Sensor List for EPSD Platforms Based on Intel® Xeon® Processor E5 4600/2600/2400/1600/1400 Product Families

Specific server boards may only implement a sub-set of sensors and/or may include additional sensors. The system-specific details of supported sensors and events are described in the Appendix of this document. The actual sensor name associated with a sensor number may vary between server boards or systems.

Sensor Type Codes

Sensor table given below lists the sensor identification numbers and information regarding the sensor type, name, supported thresholds, assertion and de-assertion information, and a brief description of the sensor purpose. Refer to the *Intelligent Platform Management Interface Specification, Version 2.0* for sensor and event/reading-type table information.

- **Sensor Type**
  The sensor type references the values in the Sensor Type Codes table in the Intelligent Platform Management Interface Specification Second Generation v2.0. It provides a context to interpret the sensor.
- **Event/Reading Type**
  The event/reading type references values from the Event/Reading Type Code Ranges and the Generic Event/Reading Type Code tables in the Intelligent Platform Management Interface Specification Second Generation v2.0. Digital sensors are specific type of discrete sensors that only have two states.

- **Event Thresholds/Triggers**
  The following event thresholds are supported for threshold type sensors:

  - [u,l][nr,c,nc] upper non-recoverable, upper critical, upper non-critical, lower non-recoverable, lower critical, lower non-critical uc, lc upper critical, lower critical

  Event triggers are supported event-generating offsets for discrete type sensors. The offsets can be found in the *Generic Event/Reading Type Code* or *Sensor Type Code* tables in the *Intelligent Platform Management Interface Specification Second Generation,* Version 2.0*,* depending on whether the sensor event/reading type is generic or a sensor-specific response.

- **Assertion/Deassertion**
  Assertion and de-assertion indicators reveal the type of events this sensor generates:
  - As: Assertion
  - De: De-assertion
- **Readable Value/Offsets**
  - Readable value indicates the type of value returned for threshold and other non-discrete type sensors.
  - Readable offsets indicate the offsets for discrete sensors that are readable by means of the *Get Sensor Reading* command. Unless otherwise indicated, event triggers are readable. Readable offsets consist of the reading type offsets that do not generate events.
- **Event Data**
  Event data is the data that is included in an event message generated by the associated sensor. For threshold-based sensors, these abbreviations are used:
  - R: Reading value
  - T: Threshold value
- **Rearm Sensors**
  The rearm is a request for the event status for a sensor to be rechecked and updated upon a transition between good and bad states. Rearming the sensors can be done manually or automatically. This column indicates the type supported by the sensor. The following abbreviations are used in the comment column to describe a sensor:
  - A: Auto-rearm
  - M: Manual rearm
  - I: Rearm by init agent
- **Default Hysteresis**
  The hysteresis setting applies to all thresholds of the sensor. This column provides the count of hysteresis for the sensor, which can be 1 or 2 (positive or negative hysteresis).
- **Criticality**
  Criticality is a classification of the severity and nature of the condition. It also controls the behavior of the front panel status LED.
- **Standby**
  Some sensors operate on standby power. These sensors may be accessed and/or generate events when the main (system) power is off, but AC power is present.

4.3.3 BMC System Management Health Monitoring

The BMC tracks the health of each of its IPMI sensors and report failures by providing a "BMC FW Health" sensor of the IPMI 2.0 sensor type Management Subsystem Health with support for the Sensor Failure offset. Only assertions should be logged into the SEL for the Sensor Failure offset. The sensor number of the failed sensor is provided in event data byte 2, as per the *IPMI 2.0 Specification.* The BMC Firmware Health sensor asserts for any sensor when 10 consecutive sensor errors are read. These are not standard sensor events (i.e. threshold crossings or discrete assertions). These are BMC Hardware Access Layer (HAL) errors like I2C NAKs or internal errors while attempting to read a register. If a successful sensor read is completed, the counter resets to zero.

IPMI Sensor Characteristics

1. Event reading type code: 6Fh (Sensor specific)
2. Sensor type code: 28h (Management Subsystem Health)
3. Rearm type: Auto

If this sensor is implemented, then the following sensor-specific offsets are supported.

Table 14. Supported BMC FW Health Sensor Offsets

Offset	Description	Event Logging
04h	Sensor failure	Assertion and deassertion

4.3.4 Processor Sensors

The BMC provides IPMI sensors for processors and associated components, such as voltage regulators and fans. The sensors are implemented on a per-processor basis.

Table 15. Processor Sensors

Sensor Name	Per-Processor Socket	Description
Processor Status	Yes	Processor presence and fault state
Digital Thermal Sensor	Yes	Relative temperature reading by means of PECI
Processor VRD Over-Temperature Indication	Yes	Discrete sensor that indicates a processor VRD has crossed an upper operating temperature threshold
Processor Voltage	Yes	Threshold sensor that indicates a processor power-good state
Processor Thermal Control (Prochot)	Yes	Percentage of time a processor is throttling due to thermal conditions

4.3.4.1 Processor Status Sensors

The BMC provides an IPMI sensor of type processor for monitoring status information for each processor slot. If an event state (sensor offset) has been asserted, it remains asserted until one of the following happens:

1. A Rearm Sensor Events command is executed for the processor status sensor.
2. AC or DC power cycle, system reset, or system boot occurs.

The BMC provides system status indication to the front panel LEDs for processor fault conditions shown in Table 16.

CPU Presence status is not saved across AC power cycles and therefore will not generate a de-assertion after cycling AC power.

Table 16. Processor Status Sensor Implementation

Offset	Processor Status	Detected By
0	Internal error (IERR)	Not Supported
1	Thermal trip	BMC
2	FRB1/BIST failure	Not Supported
3	FRB2/Hang in POST failure	BIOS[1]
4	FRB3/Processor startup/initialization failure (CPU fails to start)	Not Supported
5	Configuration error (for DMI)	BIOS[1]
6	SM BIOS uncorrectable CPU-complex error	Not Supported
7	Processor presence detected	BMC
8	Processor disabled	Not Supported
9	Terminator presence detected	Not Supported

Note: Fault is not reflected in the processor status sensor.

4.3.4.1.1 Processor Presence

Upon BMC initialization, which occurs when AC power is applied or the BMC is reset, the processor presence offset is initialized to the deasserted state and then the BMC checks to see if the processor is present and sets the presence offset accordingly.

This state is updated at each DC power-on and at system resets. The net effect of this is that there should be one event logged at BMC startup for processor presence for each installed processor, assuming the SDR is configured to generate the event. No additional events for processor presence are expected unless the sensor is manually re-armed using an IPMI command or a processor is removed or inserted. Note that removal and insertion should only occur when AC power is removed from the system so it is not expected that a SEL entry will be seen for this specific occurrence.

4.3.4.2 Processor Population Fault (CPU Missing) Sensor

The BMC supports a *Processor Population Fault* sensor for monitoring for the condition in which processor slots are not populated as required by the platform HW to allow power-on of the system.
At BMC startup, the BMC will check for the fault condition and set the sensor state accordingly. The BMC also checks for this fault condition at each attempt to DC power-on the system. At each DC power-on attempt, a beep code is generated if this fault is detected. Please refer Table 9 (BMC Beep Codes) for beep code details.
The following steps are used to correct the fault condition and clear the sensor state:

1. AC power down the server.
2. Install the missing processor into the correct slot.
3. AC power on the server.

Refer to the applicable platform BMC EPS as to the details of what population rules must be followed.

4.3.4.3 ERR2 Timeout Monitoring

The BMC supports an ERR2 Timeout Sensor (1 per CPU) that asserts if a CPU's ERR2 signal has been asserted for longer than a fixed time period (> 90 seconds). ERR[2] is a processor signal that indicates when the IIO (Integrated IO module in the processor) has a fatal error which could not be communicated to the core to trigger SMI. ERR[2] events are fatal error conditions, where the BIOS and OS will attempt to gracefully handle error, but may not be always do so reliably. A continuously asserted ERR2 signal is an indication that the BIOS cannot service the condition that caused the error. This is usually because that condition prevents the BIOS from running.

When an ERR2 timeout occurs, the BMC asserts/deasserts the ERR2 Timeout Sensor, and logs a SEL event for that sensor. The default behavior for BMC core firmware is to initiate a system reset upon detection of an ERR2 timeout. The BIOS setup utility provides an option to disable or enable system reset by the BMC for detection of this condition.

IPMI Sensor Characteristics

1. Event reading type code: 03h (Generic – digital discrete)
2. Sensor type code: 07h (Processor)
3. Rearm type: Auto

Table 17. Supported ERR2 Timeout Sensor Offsets

Offset	Description	Event Logging
01h	State asserted	Assertion and deassertion

4.3.4.4 CATERR Sensor and Market Segment ID (MSID) Mismatch

The BMC supports a CATERR sensor for monitoring the system CATERR signal.

The CATERR signal is defined as having 3 states; high (no event), pulsed low (possibly fatal may be able to recover), and low (fatal). All processors in a system have their CATERR pins tied together. The pin is used as a communication path to signal a catastrophic system event to all CPUs. The BMC has direct access to this aggregate CATERR signal.

The BMC only monitors for the "CATERR held low" condition. A pulsed low condition is ignored by the BMC.

If a CATERR-low condition is detected, the BMC logs an error message to the SEL against the CATERR sensor and then queries each CPU to determine if it was due to an MSID mismatch condition. An MSID mismatch occurs if a processor is installed into a system board that has incompatible power capabilities. The MSID mismatch condition is indicated in a processor machine check MSR. If PECI is non-functional (it isn't guaranteed in this situation), then MSID mismatch can't be detected in that case.

If the CATERR is due to an MSID mismatch, then the BMC will log an additional SEL log against the MSID Mismatch sensor, light the CPU fault LED, emit a beep code, and let the system hang. Please refer Table 9 (BMC Beep Codes) for beep code details. If no MSID

mismatch is detected, then the default action after logging the SEL entry is to reset the system. The BIOS setup utility provides an option to disable or enable system reset by the BMC for detection of this condition.

4.3.4.5 CATERR Sensor

The BMC supports a CATERR sensor for monitoring the system CATERR signal.

The sensor is rearmed on power-on (AC or DC power on transitions). It is not rearmed on system resets in order to avoid multiple SEL events that could occur due to a potential reset loop if the CATERR keeps recurring, which would be the case if the CATERR was due to an MSID mismatch condition.

On EPSD boards, the CATERR signal from each CPU are tied together and routed to the BMC as one signal. When the BMC detects that this aggregate CATERR signal has asserted, it can then go through PECI to query each CPU to determine which one was the source of the error and write an OEM code identifying the CPU slot into an event data byte in the SEL entry. If PECI is non-functional (it isn't guaranteed in this situation), then the OEM code should indicate that the source is unknown.

Event data byte 2 and byte 3 for CATERR sensor SEL events

ED2 - CATERR type.
0: Unknown
1: CATERR
2: CPU Core Error (not supported on EPSD Platforms Based on Intel® Xeon® Processor E5 4600/2600/2400/1600 Product Families)
3: MSID Mismatch

ED3 - CPU bitmap that causes the system CATERR.
[0]: CPU0
[1]: CPU1
[2]: CPU2
[3]: CPU3

IPMI Sensor Characteristics

1. Event reading type code: 03h (Digital discrete)
2. Sensor type code: 07h (Processor)
3. Rearm type: Manual

The following sensor-specific offsets are supported:

Table 18. Supported CATERR Sensor Offsets

Offset	Description	Event Logging
01h	State asserted	Assertion and deassertion

4.3.4.6 MSID Mismatch Sensor

The BMC supports a *MSID Mismatch* sensor for monitoring for the fault condition that will occur if there is a power rating incompatibility between a baseboard and an a processor

The sensor is rearmed on power-on (AC or DC power on transitions).

IPMI Sensor Characteristics

1. Event reading type code: 03h (Digital discrete)
2. Sensor type code: 07h (Processor)
3. Rearm type: Manual

The following sensor-specific offsets are supported:

Table 19. Support MSID Mismatch Sensor Offsets

Offset	Description	Event Logging
01h	State asserted	Assertion and deassertion

4.3.5 Thermal and Acoustic Management

This feature refers to enhanced fan management to keep the system optimally cooled while reducing the amount of noise generated by the system fans. Aggressive acoustics standards might require a trade-off between fan speed and system performance parameters that contribute to the cooling requirements, primarily memory bandwidth. The BIOS, BMC, and SDRs work together to provide control over how this trade-off is determined.

This capability requires the BMC to access temperature sensors on the individual memory DIMMs. Additionally, closed-loop thermal throttling is only supported with buffered DIMMs.

4.3.6 Thermal Sensor Input to Fan Speed Control

The BMC uses various IPMI sensors as input to the fan speed control. Some of the sensors are IPMI models of actual physical sensors whereas some are “virtual” sensors whose values are derived from physical sensors using calculations and/or tabular information.

The following IPMI thermal sensors are used as input to the fan speed control:

- Front panel temperature sensor
- Baseboard temperature sensors
- CPU DTS-Spec margin sensors
- DIMM thermal margin sensors
- Exit air temperature sensor
- Global aggregate thermal margin sensors
- SSB (Patsburg) temperature sensor
- On-board Ethernet controller temperature sensors (support for this is specific to the Ethernet controller being used)
- Add-in Intel SAS/IO module temperature sensor(s) (if present)
- Power supply thermal sensors (only available on PMBus-compliant power supplies).

A simple model is shown in the following figure which gives a high level graphic of the fan speed control structure creates the resulting fan speeds.

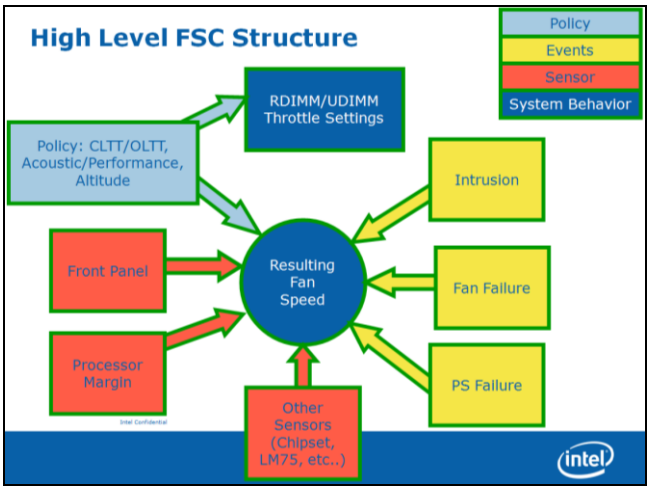


Figure 25. High-level Fan Speed Control Process

4.3.6.1.1 Processor Thermal Management

Processor thermal management utilizes clamp algorithms for which the Processor DTS-Spec margin sensor is a controlling input. This replaces the use of the (legacy) raw DTS sensor reading that was utilized on previous generation platforms. The legacy DTS sensor is retained only for monitoring purposes and is not used as an input to the fan speed control.

4.3.6.1.2 Memory Thermal Management

The system memory is the most complex subsystem to thermally manage as it requires substantial interactions between the BMC, BIOS, and the embedded memory controller HW. This section provides an overview of this management capability from a BMC perspective.

4.3.6.1.2.1 Memory Thermal Throttling

The system shall support thermal management through open loop throttling (OLTT) and closed loop throttling (CLTT) of system memory based on the platform as well as availability of valid temperature sensors on the installed memory DIMMs. Throttling levels are changed dynamically to cap throttling based on memory and system thermal conditions as determined by the system and DIMM power and thermal parameters. Support for CLTT on mixed-mode DIMM populations (i.e. some installed DIMMs have valid temp sensors and some do not) is not supported. The BMC fan speed control functionality is related to the memory throttling mechanism used.
The following terminology is used for the various memory throttling options:

- Static Open Loop Thermal Throttling (Static-OLTT): OLTT control registers are configured by BIOS MRC remain fixed after post. The system does not change any of the throttling control registers in the embedded memory controller during runtime.
- Static Closed Loop Thermal Throttling (Static-CLTT): CLTT control registers are configured by BIOS MRC during POST. The memory throttling is run as a closed-loop system with the DIMM temperature sensors as the control input. Otherwise, the system does not change any of the throttling control registers in the embedded memory controller during runtime.
- Dynamic Open Loop Thermal Throttling (Dynamic-OLTT): OLTT control registers are configured by BIOS MRC during POST. Adjustments are made to the throttling during runtime based on changes in system cooling (fan speed).

- Dynamic Closed Loop Thermal Throttling (Dynamic-CLTT): CLTT control registers are configured by BIOS MRC during POST. The memory throttling is run as a closed-loop system with the DIMM temperature sensors as the control input. Adjustments are made to the throttling during runtime based on changes in system cooling (fan speed).

4.3.6.1.2.2 Memory Thermal Throttling

Romley introduces a new type of CLTT which is referred to as Hybrid CLTT for which the Integrated Memory Controller estimates the DRAM temperature in between actual reads of the TSODs. Hybrid CLTTT shall be used on all EPSD Romley systems that have DIMMs with thermal sensors. Therefore, the terms Dynamic-CLTT and Static-CLTT are really referring to this 'hybrid' mode. Note that if the IMC's polling of the TSODs is interrupted, the temperature readings that the BMC gets from the IMC shall be these estimated values.

4.3.6.1.3 DIMM Temperature Sensor Input to Fan Speed Control

A clamp algorithm is used for controlling fan speed based on DIMM temperatures. Aggregate DIMM temperature margin sensors are used as the control input to the algorithm.

4.3.6.1.4 Dynamic (Hybrid) CLTT

The system will support dynamic (memory) CLTT for which the BMC FW dynamically modifies thermal offset registers in the IMC during runtime based on changes in system cooling (fan speed). For static CLTT, a fixed offset value is applied to the TSOD reading to get the die temperature; however this is does not provide as accurate results as when the offset takes into account the current airflow over the DIMM, as is done with dynamic CLTT.

In order to support this feature, the BMC FW will derive the air velocity for each fan domain based on the PWM value being driven for the domain. Since this relationship is dependent on the chassis configuration, a method must be used which support this dependency (for example, from OEM SDR) that establishes a lookup table providing this relationship.

BIOS will have an embedded lookup table that provides thermal offset values for each DIMM type, altitude setting, and air velocity range (3 ranges of air velocity are supported). During system boot BIOS will provide 3 offset values (corresponding to the 3 air velocity ranges) to the BMC for each enabled DIMM. Using this data the BMC FW constructs a table that maps the offset value corresponding to a given air velocity range for each DIMM. During runtime the BMC applies an averaging algorithm to determine the target offset value corresponding to the current air velocity and then the BMC writes this new offset value into the IMC thermal offset register for the DIMM.

4.3.6.1.5 Fan Profiles

The server system supports multiple fan control profiles to support acoustic targets and American Society of Heating, Refrigerating and Air Conditioning Engineers (ASHRAE) compliance. The BIOS Setup utility can be used to choose between meeting the target acoustic level or enhanced system performance. This is accomplished through fan profiles.

The BMC supports eight fan profiles, numbered from 0 to 7. Fan management policy is dictated by the Tcontrol SDRs. These SDRs provide a way to associate fan control behavior with one or more fan profiles.

Each group of profiles allows for varying fan control policies based on the altitude. For a given altitude, the Tcontrol SDRs associated with an acoustics-optimized profile generate less noise than the equivalent performance-optimized profile by driving lower fan speeds, and the BIOS reduces thermal management requirements by configuring more aggressive memory throttling. See table below for more information.

The BMC provides commands that query for fan profile support and it provides a way to enable a fan profile. Enabling a fan profile determines which Tcontrol SDRs are used for fan management. The BMC only supports enabling a fan profile through the command if that profile is supported on all fan domains defined for the system. It is important to configure the SDRs so that all desired fan profiles are supported on each fan domain. If no single profile is supported across all domains, the BMC, by default, uses profile 0 and does not allow it to be changed.

At system boot, the BIOS can use the Get Fan Control Configuration command to query the BMC about which fan profiles are supported. The BIOS uses this information to display options in the BIOS Setup utility. The BIOS indicates the fan profile to the BMC, as dictated by the BIOS Setup Utility options for fan mode and altitude, using the Set Fan Control Configuration command.

The BMC uses this information as an input to its fan-control algorithm as supported by the Tcontrol OEM SDR. The BMC only allows enabling of fan profiles that the BMC indicates are supported using the Get Fan Control Configuration command. For example, if the Get Fan Control Configuration command indicates that only profile 1 is supported, then using the Set Fan Control Configuration command to enable profile 2 will result in the return of an error completion code.

The BMC requires the BIOS to send the Set Fan Control Configuration command to the BMC on every system boot. This must be done after the BIOS has completed any throttling-related chipset configuration.

Table 20. Fan Profile Mapping

Type	Profile	Details
OLTT	0	Acoustic, 300M altitude
OLTT	1	Performance, 300M altitude
OLTT	2	Acoustic, 900M altitude
OLTT	3	Performance, 900M altitude
OLTT	4	Acoustic, 1500M altitude
OLTT	5	Performance, 1500M altitude
OLTT	6	Acoustic, 3000M altitude
OLTT	7	Performance, 3000M altitude
CLTT	0	300M altitude
CLTT	2	900M altitude
CLTT	4	1500M altitude
CLTT	6	3000M altitude

4.3.6.1.6 Open-Loop Thermal Throttling Fallback

Normal system operation uses closed-loop thermal throttling (CLTT) and DIMM temperature monitoring as major factors in overall thermal and acoustics management. In the event that BIOS is unable to configure the system for CLTT, it defaults to open-loop thermal throttling

(OLTT). In the OLTT mode, it is assumed that the DIMM temperature sensors are not available for fan speed control. The BIOS communicates the throttling mode to the BMC along with the fan profile number when it sends the *Set Fan Control Configuration* command.

When OLTT mode is specified, the BMC internally blocks access to the DIMM temperatures, causing the DIMM aggregate margin sensors to be marked as *Reading/State Unavailable*. The BMC then uses the failure-control values for these sensors, if specified in the Tcontrol SDRs, as their fan speed contributions. The system thermal engineers should configure the failure-control values so that they provide the desired cooling guard-band when the system is operating in the OLTT mode.

4.3.7 Power Supply Status\Health Sensors

The BMC supports one Power Supply Status sensor for each system power supply module. In order to track problems in which the PSU firmware is not operating to full capacity, an additional case (degraded condition if the PSU firmware is not operating to full capacity) is added to the existing Power Supply Status sensor offset definitions. This is handled by assertion of the "configuration error" offset of the PSU status sensor. These sensors are only supported for systems that use PMBus-compliant power supplies.

IPMI Sensor Characteristics

1. Event reading type code: 6Fh (Sensor Specific)
2. Event sensor type code: 08h (Power Supply)
3. Rearm type: Auto

The following sensor-specific offsets are supported.

Table 21. Supported Power Supply Status Sensor Offsets

Offset	Description	Event Logging
00h	Presence detected – Asserted if power supply module is present. Events are only logged for power supply presence upon changes in the presence state after AC power is applied (no events logged for initial state).	Assertion and Deassertion
01h	Power supply failure detected – Asserted if power supply module has failed. The following codes for failure modes are put into the SEL Event Data 2 byte: ▪ 01h - Output voltage fault ▪ 02h - Output power fault ▪ 03h - Output over-current fault ▪ 04h - Over-temperature fault ▪ 05h – Fan fault The SEL Event Data 3 byte will have the contents of the associated PMBus Status register to allow for showing multiple conditions for the event. For example, Data 3 will have the contents of the VOLTAGE_STATUS register at the time an Output Voltage fault was detected. Refer to the *PMBus Specification* for details on specific resister contents	Assertion and Deassertion

Offset	Description	Event Logging
02h	Predictive failure – Asserted if some condition, such as failing fan, has been detected that is likely to lead to a power supply module failure. The following codes for warning modes are put into the SEL Event Data 2 byte: ▪ 01h - Output voltage warning ▪ 02h - Output power warning ▪ 03h - Output over-current warning ▪ 04h - Over-temperature warning ▪ 05h - Fan warning ▪ 06h - Under-voltage warning ▪ 07h - Input over-current warning ▪ 08h - Input over-power warning The SEL Event Data 3 byte will have the contents of the associated PMBus Status register to allow for showing multiple conditions for the event. For example, Data 3 will have the contents of the VOLTAGE_STATUS register at the time an Output Voltage Warning was detected. Refer to the PMBus Specification for details on specific resister contents.	Assertion and Deassertion
03h	Power supply AC lost – Asserted if there is no AC power input to power supply module.	Assertion and Deassertion
06h	Configuration error – The following codes for configuration errors are put into the SEL Event Data 2 byte: ▪ 01h - The BMC cannot access the PMBus device on the PSU but its FRU device is responding. ▪ 02h - The PMBUS_REVISION command returns a version number that is not supported (only version 1.1 and 1.2 are supported for platforms covered under this FW EAS). ▪ 03h - The PMBus device does not successfully respond to the PMBUS_REVISION command. ▪ 04h – The PSU is incompatible with one or more PSUs that are present in the system. 05h –The PSU FW is operating in a degraded mode (likely due to a failed firmware update).	Assertion and Deassertion

4.3.8 System Event Sensor

The BMC supports a System Event sensor and logs SEL event for following events.

Table 22. Support System Event Sensor Offsets

Offset	Description	Event Logging
02h	OEM code (Undetermined system HW failure)	Assertion and Deassertion
04h	PEF action	Assertion only

For offset 2, OEM code will be logged in event data byte 2 to indicate the type of failure. Only one value will be supported at this time, but others may be added in the future. The code for this particular fault will be 0x00 (PECI access failure) and all other values reserved. Upon detection of the CPU PECI fault condition, the offset shall assert. It shall deassert upon system power cycle or system reset. Assertion of offset 02h shall contribute a “fatal” condition to the system status as reflected in the Front Panel system status LED.

4.3.8.1 Update Related SEL Logging

BMC FW will support a single FW Update Status sensor. This sensor is used to generate SEL events related to update of embedded firmware on the platform. This includes updates to the BMC, BIOS, and ME FW.

IPMI Sensor Characteristics

1. Event reading type code: 70h (OEM defined)
2. Sensor type code: 2Bh (Version Change)
3. Rearm type: Auto

This sensor is an event-only sensor that is not readable. Event generation is only enabled for assertion events. Since this is an event-only sensor it should be defined by a type-3 SDR as defined in the IPMI 2.0 Specification.

Table 23. Supported Firmware Update Status Sensor Offsets

Offset	Description	Event Logging	Contribution to system health
00h	Update started	Assertion	OK
01h	Update completed successfully	Assertion	OK
02h	Update failure	Assertion	OK

Event Data Bytes

Byte 2: [Bits 7:4] Target of update

0000b = BMC

0001b = BIOS

0010b = ME

0011b = EWS (Embedded Web server)

All other values reserved

[Bits 3:1] Target instance (zero-based)

[Bits 0:0] Reserved

Byte 3: Reserved

Note: All reserved bits must be set to zero.

4.4 Platform Management Interface

This chapter describes the supported BMC communication interfaces:

1. Host SMS interface by means of low pin count (LPC)/keyboard controller style (KCS) interface
2. Host SMM interface by means of low pin count (LPC)/keyboard controller style (KCS) interface
3. Intelligent Platform Management Bus (IPMB) I2C interface
4. LAN interface using the IPMI-over-LAN protocols

4.4.1 Channel Management

Every messaging interface is assigned an IPMI channel ID by IPMI 2.0. Commands are provided to configure each channel for privilege levels and access modes. Table 24 shows the standard channel assignments:

Table 24. Standard Channel Assignments

Channel ID	Interface	Supports Sessions
0	Primary IPMB	No
1	LAN 1	Yes
2	LAN 2	Yes
3	LAN3 [1] (Provided by the Intel® Dedicated Server Management NIC)	Yes
4	Reserved	Yes
5	USB	No
6	Secondary IPMB	No
7	SMM	No
8 – 0Dh	Reserved	–
0Eh	Self [2]	–
0Fh	SMS/Receive Message Queue	No

Notes:

1. Optional hardware supported by the server system.
2. Refers to the actual channel used to send the request.

4.4.2 User Model

The BMC supports the IPMI 2.0 user model. 15 user IDs are supported. These 15 users can be assigned to any channel. The following restrictions are placed on user-related operations:

1. User names for User IDs 1 and 2 cannot be changed. These are always “” (Null/blank) and “root” respectively.
2. User 2 (“root”) always has the administrator privilege level.
3. All user passwords (including passwords for 1 and 2) may be modified.
4. User IDs 3-15 may be used freely, with the condition that user names are unique. Therefore, no other users can be named “” (Null), “root,” or any other existing user name.

4.4.3 LAN Interface

The BMC implements both the IPMI 1.5 and IPMI 2.0 messaging models. These provide out-of-band local area network (LAN) communication between the BMC and the network.

Run-time determination of LAN channel capabilities can be determined by both standard IPMI defined mechanisms.

4.4.3.1 IPMI 1.5 Messaging

The communication protocol packet format consists of IPMI requests and responses encapsulated in an IPMI session wrapper for authentication, and wrapped in an RMCP packet, which is wrapped in an IP/UDP packet. Although authentication is provided, no encryption is provided, so administrating some settings, such as user passwords, through this interface is not advised. Session establishment commands are IPMI commands that do not require authentication or an associated session.

The BMC supports the following authentication types over the LAN interface.

1. None (no authentication)
2. Straight password/key
3. MD5

4.4.3.2 IPMI 2.0 Messaging

IPMI 2.0 messaging is built over RMCP+ and has a different session establishment protocol. The session commands are defined by RMCP+ and implemented at the RMCP+ level, not IPMI commands. Authentication is implemented at the RMCP+ level. RMCP+ provides link payload encryption, so it is possible to communicate private/sensitive data (confidentiality).

The BMC supports the cipher suites identified in Table 25.

Table 25. Supported RMCP+ Cipher Suites

ID	Authentication Algorithm	Integrity Algorithm(s)	Confidentiality Algorithm(s)
0[1]	RAKP-none	None	None
1	RAKP-HMAC-SHA1	None	None
2	RAKP-HMAC-SHA1	HMAC-SHA1-96	None
3	RAKP-HMAC-SHA1	HMAC-SHA1-96	AES-CBC-128
6	RAKP-HMAC-MD5	None	None
7	RAKP-HMAC-MD5	HMAC-MD5-128	None
8	RAKP-HMAC-MD5	HMAC-MD5-128	AES-CBC-128
11	RAKP-HMAC-MD5	MD5-128	None
12	RAKP-HMAC-MD5	MD5-128	AES-CBC-128

Note: Cipher suite 0 defaults to callback privilege for security purposes. This may be changed by any administrator.

For user authentication, the BMC can be configured with ‘null’ user names, whereby password/key lookup is done based on ‘privilege level only’, or with non-null user names, where the key lookup for the session is determined by user name.

IPMI 2.0 messaging introduces payload types and payload IDs to allow data types other than IPMI commands to be transferred. IPMI 2.0 serial-over-LAN is implemented as a payload type.

Table 26. Supported RMCP+ Payload Types

Payload Type	Feature	IANA
00h	IPMI message	N/A
01h	Serial-over-LAN	N/A
02h	OEM explicit	Intel (343)
10h – 15h	Session setup	N/A

4.4.3.3 RMCP/ASF Messaging

The BMC supports RMCP ping discovery in which the BMC responds with a pong message to an RMCP/ASF ping request. This is implemented per the *Intelligent Platform Management Interface Specification Second Generation v2.0*.

4.4.3.4 BMC LAN Channels

The BMC supports three RMII/RGMII ports that can be used for communicating with Ethernet devices. Two ports are used for communication with the on-board NICs and one is used for communication with an Ethernet PHY located on an optional add-in card (or equivalent on-board circuitry).

4.4.3.4.1 Baseboard NICs

The specific Ethernet controller (NIC) used on a server is platform-specific but all baseboard device options provide support for an NC-SI manageability interface. This provides a sideband high-speed connection for manageability traffic to the BMC while still allowing for a simultaneous host access to the OS if desired.

The Network Controller Sideband Interface (NC-SI) is a DMTF industry standard protocol for the side band management LAN interface. This protocol provides a fast multi-drop interface for management traffic.

The baseboard NIC(s) are connected to a single BMC RMII/RGMII port that is configured for RMII operation. The NC-SI protocol is used for this connection and provides a 100 Mb/s full-duplex multi-drop interface which allows multiple NICs to be connected to the BMC. The physical layer is based upon RMII, however RMII is a point-to-point bus whereas NC-SI allows 1 master and up to 4 slaves. The logical layer (configuration commands) is incompatible with RMII.

Multi-port baseboard NICs on some products will provide support for a dedicated management channel than can be configured to be hidden from the host and only used by the BMC. This mode of operation is configured by a BIOS setup option.

4.4.3.4.2 Dedicated Management Channel

An additional LAN channel dedicated to BMC usage and not available to host SW is supported by an optional add-in card. There is only a PHY device present on the add-in card. The BMC has a built-in MAC module that uses the RGMII interface to link with the card's PHY. Therefore, for this dedicated management interface, the PHY and MAC are located in different devices.

The PHY on the card connects to the BMC's other RMII/RGMII interface (i.e. the one that is not connected to the baseboard NICs). This BMC port is configured for RGMII usage.

In addition to the use of an add-in card for a dedicated management channel, on systems that support multiple Ethernet ports on the baseboard, the system BIOS provides a setup option to allow one of these baseboard ports to be dedicated to the BMC for manageability purposes. When this is enabled, that port is hidden from the OS.

4.4.3.4.3 Concurrent Server Management Use of Multiple Ethernet Controllers

Provided the HW supports a management link between the BMC and a NIC port, the BMC FW supports concurrent OOB LAN management sessions for the following combination:

- Two on-board NIC ports
- One on-board NIC and the optional dedicated add-in management NIC.
- Two on-board NICs and optional dedicated add-in management NIC.

All NIC ports must be on different subnets for the above concurrent usage models.
MAC addresses are assigned for management NICs from a pool of up to 3 MAC addresses allocated specifically for manageability. The total number of MAC addresses in the pool is dependent on the product HW constraints (for example,a board with 2 NIC ports available for manageability would have a MAC allocation pool of 2 addresses).For these channels, support can be enabled for IPMI-over-LAN and DHCP.

For security reasons, embedded LAN channels have the following default settings:

IP Address: Static
All users disabled

IPMI-enabled network interfaces may not be placed on the same subnet. This includes the Intel® Dedicated Server Management NIC and either of the BMC's embedded network interfaces.

Host-BMC communication over the same physical LAN connection – also known as "loopback" – is not supported. This includes "ping" operations.

On baseboards with more than two onboard NIC ports, only the first two ports can be used as BMC LAN channels. The remaining ports have no BMC connectivity.

- Maximum bandwidth supported by BMC LAN channels are as follows:
- BMC LAN1 (Baseboard NIC port) ----- 100M (10M in DC off state)
- BMC LAN 2 (Baseboard NIC port) ----- 100M (10M in DC off state)
- BMC LAN 3 (Dedicated NIC) ----- 1000M

4.4.3.5 Dedicated Management NIC MAC Address

For EPSD Platforms Based on Intel® Xeon® Processor E5 4600/2600/2400/1600/1400 Product Families each server board has either five or seven MAC addresses assigned to it at the Intel factory. The printed MAC address is assigned to NIC1 on the server board.

If the platform has two NIC built into the main board then there will be five MAC addresses assigned as follows:

- NIC 1 MAC address (for OS usage)
- NIC 2 MAC address = NIC 1 MAC address + 1 (for OS usage)

- BMC LAN channel 1 MAC address = NIC1 MAC address + 2
- BMC LAN channel 2 MAC address = NIC1 MAC address + 3
- BMC LAN channel 3 (RMM) MAC address = NIC1 MAC address + 4

If the platform has four NIC built into the main board then there will be seven MAC addresses assigned as follows:

- NIC 1 MAC address (for OS usage)
- NIC 2 MAC address = NIC 1 MAC address + 1 (for OS usage)
- NIC 3 MAC address = NIC 1 MAC address + 2 (for OS usage)
- NIC 4 MAC address = NIC 1 MAC address + 3 (for OS usage)
- BMC LAN channel 1 MAC address = NIC1 MAC address + 4
- BMC LAN channel 2 MAC address = NIC1 MAC address + 5
- BMC LAN channel 3 (RMM) MAC address = NIC1 MAC address + 6.

4.4.3.6 IPV6 Support

In addition to IPv4, Intel® S1400/S1600/S2400/S2600 Server Platforms support IPv6 for manageability channels. Configuration of IPv6 is provided by extensions to the IPMI Set and Get LAN Configuration Parameters commands as well as through a Web Console IPv6 configuration web page.

The BMC supports IPv4 and IPv6 simultaneously so they are both configured separately and completely independently. For example, IPv4 can be DHCP configured while IPv6 is statically configured or vice versa.

4.4.3.6.1 LAN Failover

The BMC FW provides a LAN failover capability such that the failure of the system HW associated with one LAN link will result in traffic being rerouted to an alternate link. This functionality is configurable by IPMI methods as well as by the BMC's Embedded UI, allowing for user to specify the physical LAN links constitute the redundant network paths or physical LAN links constitute different network paths. BMC will support only a all or nothing" approach – that is, all interfaces bonded together, or none are bonded together.

The LAN Failover feature applies only to BMC LAN traffic. It bonds all available Ethernet devices but only one is active at a time. When enabled, If the active connection's leash is lost, one of the secondary connections is automatically configured so that it has the same IP address (the next active LAN link will be chosen randomly from the pool of backup LAN links with link status as "UP"). Traffic immediately resumes on the new active connection.
The LAN Failover enable/disable command may be sent at any time. After it has been enabled, standard IPMI commands for setting channel configuration that specify a LAN channel other than the first will return an error code.

Standard IPMI commands for getting channel configuration will return the cached settings for the inactive channels.

4.4.3.7 BMC IP Address Configuration

Enabling the BMC's network interfaces requires using the *Set LAN Configuration Parameter* command to configure LAN configuration parameter 4, *IP Address Source*.

4.4.3.8 DHCP BMC Hostname

The BMC allows setting a DHCP Hostname. DHCP Hostname can be set regardless of the IP Address source configured on the BMC. But this parameter is only used if the IP Address source is set to DHCP.

4.4.3.9 Address Resolution Protocol (ARP)

The BMC can receive and respond to ARP requests on BMC NICs. Gratuitous ARPs are supported, and disabled by default.

4.4.3.10 Virtual Local Area Network (VLAN)

The BMC supports VLAN as defined by IPMI 2.0 specifications. VLAN is supported internally by the BMC, not through switches. VLAN provides a way of grouping a set of systems together so that they form a logical network. This feature can be used to set up a management VLAN where only devices which are members of the VLAN will receive packets related to management and members of the VLAN will be isolated from any other network traffic. Please note that VLAN does not change the behavior of the host network setting, it only affects the BMC LAN communication.

LAN configuration options are now supported (by means of the Set LAN Config Parameters command, parameters 20 and 21) that allow support for 802.1Q VLAN (Layer 2). This allows VLAN headers/packets to be used for IPMI LAN sessions. VLAN ID's are entered and enabled by means of parameter 20 of the Set LAN Config Parameters IPMI command. When a VLAN ID is configured and enabled, the BMC only accepts packets with that VLAN tag/ID. Conversely, all BMC generated LAN packets on the channel include the given VLAN tag/ID. Valid VLAN ID's are 1 through 4094, VLAN ID's of 0 and 4095 are reserved, per the 802.1Q VLAN specification. Only one VLAN can be enabled at any point in time on a LAN channel. If an existing VLAN is enabled, it must first be disabled prior to configuring a new VLAN on the same LAN channel.

Parameter 21 (VLAN Priority) of the Set LAN Config Parameters IPMI command is now implemented and a range from 0-7 will be allowed for VLAN Priorities. Please note that bits 3 and 4 of Parameter 21 are considered Reserved bits.

Parameter 25 (VLAN Destination Address) of the Set LAN Config Parameters IPMI command is not supported and returns a completion code of 0x80 (parameter not supported) for any read/write of parameter 25.

If the BMC IP address source is DHCP, then the following behavior is seen:

- If the BMC is first configured for DHCP (prior to enabling VLAN), when VLAN is enabled, the BMC performs a discovery on the new VLAN in order to obtain a new BMC IP address.
- If the BMC is configured for DHCP (before disabling VLAN), when VLAN is disabled, the BMC performs a discovery on the LAN in order to obtain a new BMC IP address.

If the BMC IP address source is Static, then the following behavior is seen:

- If the BMC is first configured for static (prior to enabling VLAN), when VLAN is enabled, the BMC has the same IP address that was configured before. It is left to the management application to configure a different IP address if that is not suitable for VLAN.

- If the BMC is configure for static (prior to disabling VLAN), when VLAN is disabled, the BMC has the same IP address that was configured before. It is left to the management application to configure a different IP address if that is not suitable for LAN.

4.4.3.11 Secure Shell (SSH)

Secure Shell (SSH) connections are supported for one SMASH-CLP session to the BMC.

4.4.3.12 Serial-over-LAN (SOL 2.0)

The BMC supports IPMI 2.0 SOL.

IPMI 2.0 introduced a standard serial-over-LAN feature. This is implemented as a standard payload type (01h) over RMCP+.

Three commands are implemented for SOL 2.0 configuration.

1. *"Get SOL 2.0 Configuration Parameters"* and *"Set SOL 2.0 Configuration Parameters":* These commands are used to get and set the values of the SOL configuration parameters. The parameters are implemented on a per-channel basis.
2. *"Activating SOL":* This command is not accepted by the BMC. It is sent by the BMC when SOL is activated to notify a remote client of the switch to SOL.
3. Activating a SOL session requires an existing IPMI-over-LAN session. If encryption is used, it should be negotiated when the IPMI-over LAN session is established. Intel® Server Board S2600IP SOL sessions are supported on serial port A (COM1). Intel® Workstation Board S2600IP SOL sessions are supported on serial port B (COM2).

4.4.3.13 Platform Event Filter (PEF)

The BMC includes the ability to generate a selectable action, such as a system power-off or reset, when a match occurs to one of a configurable set of events. This capability is called *Platform Event Filtering,* or PEF. One of the available PEF actions is to trigger the BMC to send a LAN alert to one or more destinations.

The BMC supports 20 PEF filters. The first twelve entries in the PEF filter table are pre-configured (but may be changed by the user). The remaining entries are left blank, and may be configured by the user.

Table 27. Factory Configured PEF Table Entries

Event Filter Number	Offset Mask	Events
1	Non-critical, critical and non-recoverable	Temperature sensor out of range
2	Non-critical, critical and non-recoverable	Voltage sensor out of range
3	Non-critical, critical and non-recoverable	Fan failure
4	General chassis intrusion	Chassis intrusion (security violation)
5	Failure and predictive failure	Power supply failure
6	Uncorrectable ECC	BIOS

Event Filter Number	Offset Mask	Events
7	POST error	BIOS: POST code error
8	FRB2	Watchdog Timer expiration for FRB2
9	Policy Correction Time	Node Manager
10	Power down, power cycle, and reset	Watchdog timer
11	OEM system boot event	System restart (reboot)
12	Drive Failure, Predicted Failure	Hot Swap Controller

Additionally, the BMC supports the following PEF actions:

- Power off
- Power cycle
- Reset
- OEM action
- Alerts

The “Diagnostic interrupt” action is not supported.

4.4.3.14 LAN Alerting

The BMC supports sending embedded LAN alerts, called SNMP PET (Platform Event traps), and SMTP email alerts.

The BMC supports a minimum of four LAN alert destinations.

4.4.3.14.1 SNMP Platform Event Traps (PETs)

This feature enables a target system to send SNMP traps to a designated IP address by means of LAN. These alerts are formatted per the *Intelligent Platform Management Interface Specification Second Generation v2.0*. A MIB file associated with the traps is provided with the BMC firmware to facilitate interpretation of the traps by external software.

The format of the MIB file is covered under RFC 2578.

4.4.3.15 Alert Policy Table

Associated with each PEF entry is an alert policy that determines which IPMI channel the alert is to be sent. There is a maximum of 20 alert policy entries. There are no pre-configured entries in the alert policy table because the destination types and alerts may vary by user. Each entry in the alert policy table contains four bytes for a maximum table size of 80 bytes.

4.4.3.15.1 E-mail Alerting

The Embedded Email Alerting feature allows the user to receive e-mails alerts indicating issues with the server. This allows e-mail alerting in an OS-absent (for example, Pre-OS and OS-Hung) situation. This feature provides support for sending e-mail by means of SMTP, the Simple Mail Transport Protocol as defined in Internet RC 821. The e-mail alert provides a text string that describes a simple description of the event. SMTP alerting is configured using the embedded web server.

4.4.3.16 SM-CLP (SM-CLP Lite)

SMASH refers to Systems Management Architecture for Server Hardware. SMASH is defined by a suite of specifications, managed by the DMTF, that standardize the manageability interfaces for server hardware. CLP refers to Command Line Protocol. SM-CLP is defined by the *Server Management Command Line Protocol Specification (SM-CLP) ver1.0*, which is part of the SMASH suite of specifications. The specifications and further information on SMASH can be found at the DMTF website (http://www.dmtf.org/).
The BMC provides an embedded "lite" version of SM-CLP that is syntax-compatible but not considered fully compliant with the DMTF standards.

4.4.3.17 Embedded Web Server

BMC Base manageability provides an embedded web server and an OEM-customizable web GUI which exposes the manageability features of the BMC base feature set. It is supported over all on-board NICs that have management connectivity to the BMC as well as an optional dedicated add-in management NIC. At least two concurrent web sessions from up to two different users is supported. The embedded web user interface shall support the following client web browsers:

- Microsoft Internet Explorer 7.0*
- Microsoft Internet Explorer 8.0*
- Microsoft Internet Explorer 9.0*
- Mozilla Firefox 3.0*
- Mozilla Firefox 3.5*
- Mozilla Firefox 3.6*

The embedded web user interface supports strong security (authentication, encryption, and firewall support) since it enables remote server configuration and control. Embedded web server uses ports #80 and #443. The user interface presented by the embedded web user interface shall authenticate the user before allowing a web session to be initiated. Encryption using 128-bit SSL is supported. User authentication is based on user id and password.

The GUI presented by the embedded web server authenticates the user before allowing a web session to be initiated. It presents all functions to all users but grays-out those functions that the user does not have privilege to execute. (For example, if a user does not have privilege to power control, then the item shall be displayed in grey-out font in that user's UI display). The web GUI also provides a launch point for some of the advanced features, such as KVM and media redirection. These features are grayed out in the GUI unless the system has been updated to support these advanced features.

Additional features supported by the web GUI includes:

- Presents all the Basic features to the users.
- Power on/off/reset the server and view current power state.
- Displays BIOS, BMC, ME and SDR version information.
- Display overall system health.
- Configuration of various IPMI over LAN parameters for both IPV4 and IPV6
- Configuration of alerting (SNMP and SMTP).
- Display system asset information for the product, board, and chassis.
- Display of BMC-owned sensors (name, status, current reading, enabled thresholds), including color-code status of sensors.

- Provides ability to filter sensors based on sensor type (Voltage, Temperature, Fan and Power supply related)
- Automatic refresh of sensor data with a configurable refresh rate.
- On-line help.
- Display/clear SEL (display is in easily understandable human readable format).
- Supports major industry-standard browsers (Microsoft Internet Explorer* and Mozilla Firefox*).
- The GUI session automatically times-out after a user-configurable inactivity period. By default, this inactivity period is 30 minutes.
- Embedded Platform Debug feature - Allow the user to initiate a “diagnostic dump” to a file that can be sent to Intel for debug purposes.
- Virtual Front Panel. The Virtual Front Panel provides the same functionality as the local front panel. The displayed LEDs match the current state of the local panel LEDs. The displayed buttons (for example,power button) can be used in the same manner as the local buttons.
- Display of ME sensor data. Only sensors that have associated SDRs loaded will be displayed.
- Ability to save the SEL to a file.
- Ability to force HTTPS connectivity for greater security. This is provided through a configuration option in the UI.
- Display of processor and memory information as is available over IPMI over LAN.
- Ability to get and set Node Manager (NM) power policies.
- Display of power consumed by the server.
- Ability to view and configure VLAN settings.
- Warn user the reconfiguration of IP address will cause disconnect.
- Capability to block logins for a period of time after several consecutive failed login attempts. The lock-out period and the number of failed logins that initiates the lock-out period are configurable by the user.
- Server Power Control - Ability to force into Setup on a reset.

4.4.3.18 Virtual Front Panel

- Virtual Front Panel is the module present as “Virtual Front Panel” on the left side in the embedded web server when "remote Control" tab is clicked.
- Main Purpose of the Virtual Front Panel is to provide the front panel functionality virtually.
- Virutal Front Panel (VFP) will mimic the status LED and Power LED status and Chassis ID alone. It is automatically in sync with BMC every 40 seconds.
- For any abnormal status LED state, Virtual Front Panel will get the reason behind the abnormal or status LED changes and displayed in VFP side.
- As Virtual Front Panel uses the chassis control command for power actions. It won’t log the Front button press event since Logging the front panel press event for Virtual Front Panel press will mislead the administrator.
- For Reset from Virtual Front Panel, the reset will be done by a “Chassis control” command.
- For Reset from Virtual Front Panel, the restart cause will be because of “Chassis control” command.
- During Power action, Power button/Reset button should not accept the next action until current Power action is complete and the acknowledgment from BMC is received.
- EWS will provide a valid message during Power action until it completes the current Power action.

- The VFP does not have any effect on whether the front panel is locked by “Set Front Panel Enables” command.
- The chassis ID LED provides a visual indication of a system being serviced. The state of the chassis ID LED is affected by the following actions:
- Toggled by turning the chassis ID button on or off.
- There is no precedence or lock-out mechanism for the control sources. When a new request arrives, previous requests are terminated. For example, if the chassis ID button is pressed, then the chassis ID LED changes to solid on. If the button is pressed again, then the chassis ID LED turns off.
- Note that the chassis ID will turn on because of the original chassis ID button press and will reflect in the Virtual Front Panel after VFP sync with BMC. Virtual Front Panel won’t reflect the chassis LED software blinking by the software command as there is no mechanism to get the chassis ID Led status.
- Only Infinite chassis ID ON/OFF by the software command will reflect in EWS during automatic /manual EWS sync up with BMC.
- Virtual Front Panel help should available for virtual panel module.
- At present, NMI button in VFP is disabled in Intel® S1400/S1600/S2400/S2600 Server Platforms. It can be used in future.

4.4.3.19 Embedded Platform Debug

The Embedded Platform Debug feature supports capturing low-level diagnostic data (applicable MSRs, PCI config-space registers, and so on). This feature allows a user to export this data into a file that is retrievable from the embedded web GUI, as well as through host and remote IPMI methods, for the purpose of sending to an Intel engineer for an enhanced debugging capability. The files are compressed, encrypted, and password protected. The file is not meant to be viewable by the end user but rather to provide additional debugging capability to an Intel support engineer.

4.4.3.20 Data Center Management Interface (DCMI)

The DCMI Specification is an emerging standard that is targeted to provide a simplified management interface for Internet Portal Data Center (IPDC) customers. It is expected to become a requirement for server platforms which are targeted for IPDCs. DCMI is an IPMI-based standard that builds upon a set of required IPMI standard commands by adding a set of DCMI-specific IPMI OEM commands. Intel® S1400/S1600/S2400/S2600 Server Platforms will be implementing the mandatory DCMI features in the BMC firmware (DCMI 1.1 Errata 1 compliance). Please refer to DCMI 1.1 errata 1 spec for details. Only mandatory commands will be supported. No support for optional DCMI commands. Optional power management and SEL roll over feature is not supported. DCMI Asset tag will be independent of baseboard FRU asset Tag. Please refer table DCMI Group Extension Commands for more details on DCMI commands.

4.4.3.21 Lightweight Directory Authentication Protocol (LDAP)

The Lightweight Directory Access Protocol (LDAP) is an application protocol supported by the BMC for the purpose of authentication and authorization. The BMC user connects with an LDAP server for login authentication. This is only supported for non-IPMI logins including the embedded web UI and SM-CLP. IPMI users/passwords and sessions are not supported over LDAP.

LDAP can be configured (IP address of LDAP server, port, and so on) from the BMC's Embedded Web UI. LDAP authentication and authorization is supported over the any NIC configured for system management. The BMC uses a standard Open LDAP implementation for Linux.

Only open LDAP is supported by BMC. Windows and Novel LDAP are not supported.

4.5 BMC Firmware Update

4.5.1 The BMC firmware release Number

The BMC firmware releases are numbered as follows:

AB.CD.XXX

Where:

CD is a two digit number starting with 00 for the first release. This is the number returned in minor ID in Get Device ID response.

B is major release number (1 for the first major release typically at first production shipment).

A is point release indicator (A=0 means this is a regular official release, A=1 means this is a point release for limited distribution). A hex representation of "AB" is returned in major ID in Get Device ID response.

XXX is the build number for internal tracking. This number is returned in OEM bytes of Get Device ID response.

4.5.2 Boot Recovery Mode

The BMC's boot block supports firmware transfer updates. The Operational Firmware Transfer mode preserves several files in the PIA Linux file system. Boot Recovery mode cannot preserve the files because it does not understand Linux file systems, and treats it as a large binary data section. This means a Boot Recovery update completely replaces the PIA with the factory default version: an empty SEL, a default SDR, and default IPMI configuration and user settings.

Boot Recovery mode can successfully complete an update in some situations where the Operational Firmware Transfer mode will fail. If there is an incompatibility or bug in the operational code causing it to crash or hang, only a Boot Recovery Mode Update works. Another example is if the flash layout of the sections changes across an update. Because the operational Firmware Transfer mode tries to preserve the contents of the PIA section, in this case, it will corrupt the flash where the old PIA section was. Because the Boot Recovery mode is blindly writing binary data to flash, in this case, it will succeed.

There are two ways to enter Boot Recovery mode:

- The Force Firmware Update jumper is asserted when A/C power is applied.
- The operational code is corrupt and the boot loader cannot boot.

In the Boot Recovery mode, the BMC only responds to the small set of commands listed above. Only the KCS SMS interface is supported; USB-based Fast Firmware Update is not supported.

4.5.3 Force Firmware Update Jumper

The Force Firmware Update jumper can be used to put the BMC in Boot Recovery mode for a low-level update. It causes the BMC to abort its normal boot process and stay in the boot loader without executing any Linux code.

The jumper is normally in the de-asserted position. The system must be completely powered off (A/C power removed) before the jumper is moved. After power is re-applied and the firmware update is complete, the system must be powered off again and the jumper must be returned to the de-asserted position before normal operation can begin.

There is no boot–block-write protection jumper.

4.5.4 Fast Firmware Update over USB

The BMC supports a Fast Firmware Update mode in addition to the standard KCS SMS interface. This is a special protocol that goes over the USB connection between the host and the BMC.

4.6 Advanced Management Feature Support

This section explains the advanced management features supported by the BMC firmware.

4.6.1 Enabling Advanced Management Features

The *Advanced* management features are to be delivered as part of the BMC FW image. The BMC's baseboard SPI flash contains code/data for both the *Basic* and *Advanced* features. An optional add-in card Intel® RMM4 lite is used as the activation mechanism. When the BMC FW initializes, it attempts to access the Intel® RMM4 lite. If the attempt to access Intel® RMM4 lite is successful, then the BMC activates the *Advanced* features.

Advanced manageability features are supported over all NIC ports enabled for server manageability. This includes baseboard NICs as well as the LAN channel provided by the optional Dedicated NIC add-in card.

RMM4 is comprised of two boards – RMM4 lite and the optional Dedicated Server Management NIC (DMN). If the optional Dedicated Server Management NIC is not used then the traffic can only go through the onboard Integrated BMC-shared NIC and share network bandwidth with the host system.

Table 28. Enabling Advanced Management Features

Manageability Hardware	Benefits
Intel® Integrated BMC	Comprehensive IPMI based base manageability features
Intel® Remote Management Module 4 – Lite Package contains one module – 1- Key for advance Manageability features.	No dedicated NIC for management Enables KVM and media redirection from the onboard NIC
Intel® Remote Management Module 4 Package includes 2 modules – 1 - key for advance features 2 - Dedicated NIC (1Gbe) for management	Dedicated NIC for management traffic. Higher bandwidth connectivity for KVM and media Redirection with 1Gbe NIC.

4.6.2 Keyboard, Video, Mouse (KVM) Redirection

The BMC firmware supports keyboard, video, and mouse redirection (KVM) over LAN. This feature is available remotely from the embedded web server as a Java applet. This feature is only enabled when the Intel® RMM4 lite is present. The client system must have a Java Runtime Environment (JRE) version 6.0 or later to run the KVM or media redirection applets.

The BMC supports an embedded KVM application (Remote Console) that can be launched from the embedded web server from a remote console. USB1.1 or USB 2.0 based mouse and keyboard redirection are supported. It is also possible to use the KVM-redirection (KVM-r) session concurrently with media-redirection (media-r). This feature allows a user to interactively use the keyboard, video, and mouse (KVM) functions of the remote server as if the user were physically at the managed server.

KVM redirection console support the following keyboard layouts: English, Dutch, French, German, Italian, Russian, and Spanish.
KVM redirection includes a “soft keyboard” function. The “soft keyboard” is used to simulate an entire keyboard that is connected to the remote system. The “soft keyboard” functionality supports the following layouts: English, Dutch, French, German, Italian, Russian, and Spanish.
The KVM-redirection feature automatically senses video resolution for best possible screen capture and provides high-performance mouse tracking and synchronization. It allows remote viewing and configuration in pre-boot POST and BIOS setup, once BIOS has initialized video.
Other attributes of this feature include:

- Encryption of the redirected screen, keyboard, and mouse
- Compression of the redirected screen.
- Ability to select a mouse configuration based on the OS type.
- supports user definable keyboard macros.

KVM redirection feature supports the following resolutions and refresh rates:

- 640x480 at 60Hz, 72Hz, 75Hz, 85Hz, 100Hz
- 800x600 at 60Hz, 72Hz, 75Hz, 85Hz
- 1024x768 at 60Hx, 72Hz, 75Hz, 85Hz
- 1280x960 at 60Hz
- 1280x1024 at 60Hz
- 1600x1200 at 60Hz
- 1920x1080 (1080p),
- 1920x1200 (WUXGA)
- 1650x1080 (WSXGA+)

4.6.2.1 Force-enter BIOS Setup

KVM redirection can present an option to force-enter BIOS Setup. This enables the system to enter F2 setup while booting which is often missed by the time the remote console redirects the video.

4.6.3 Media Redirection

The embedded web server provides a Java applet to enable remote media redirection. This may be used in conjunction with the remote KVM feature, or as a standalone applet.

The media redirection feature is intended to allow system administrators or users to mount a remote IDE or USB CD-ROM, floppy drive, or a USB flash disk as a remote device to the server. Once mounted, the remote device appears just like a local device to the server, allowing system administrators or users to install software (including operating systems), copy files, update BIOS, and so on, or boot the server from this device.

The following capabilities are supported:

- The operation of remotely mounted devices is independent of the local devices on the server. Both remote and local devices are useable in parallel.
- Either IDE (CD-ROM, floppy) or USB devices can be mounted as a remote device to the server.
- It is possible to boot all supported operating systems from the remotely mounted device and to boot from disk IMAGE (*.IMG) and CD-ROM or DVD-ROM ISO files. See the Tested/supported Operating System List for more information.

- Media redirection supports redirection for both a virtual CD device and a virtual Floppy/USB device concurrently. The CD device may be either a local CD drive or else an ISO image file; the Floppy/USB device may be either a local Floppy drive, a local USB device, or else a disk image file.
- The media redirection feature supports multiple encryption algorithms, including RC4 and AES. The actual algorithm that is used is negotiated with the client based on the client's capabilities.
- A remote media session is maintained even when the server is powered-off (in standby mode). No restart of the remote media session is required during a server reset or power on/off. An BMC reset (for example,due to an BMC reset after BMC FW update) will require the session to be re-established
- The mounted device is visible to (and useable by) managed system's OS and BIOS in both pre-boot and post-boot states.
- The mounted device shows up in the BIOS boot order and it is possible to change the BIOS boot order to boot from this remote device.
- It is possible to install an operating system on a bare metal server (no OS present) using the remotely mounted device. This may also require the use of KVM-r to configure the OS during install.

USB storage devices will appear as floppy disks over media redirection. This allows for the installation of device drivers during OS installation.

If either a virtual IDE or virtual floppy device is remotely attached during system boot, both the virtual IDE and virtual floppy are presented as bootable devices. It is not possible to present only a single-mounted device type to the system BIOS.

4.7 Intel® Intelligent Power Node Manager (NM)

4.7.1 Overview

Power management deals with requirements to manage processor power consumption and manage power at the platform level to meet critical business needs. Node Manager (NM) is a platform resident technology that enforces power capping and thermal-triggered power capping policies for the platform. These policies are applied by exploiting subsystem knobs (such as processor P and T states) that can be used to control power consumption. NM enables data center power management by exposing an external interface to management software through which platform policies can be specified. It also implements specific data center power management usage models such as power limiting, and thermal monitoring.

The NM feature is implemented by a complementary architecture utilizing the ME, BMC, BIOS, and an ACPI-compliant OS. The ME provides the NM policy engine and power control/limiting functions (referred to as Node Manager or NM) while the BMC provides the external LAN link by which external management software can interact with the feature. The BIOS provides system power information utilized by the NM algorithms and also exports ACPI Source Language (ASL) code used by OS-Directed Power Management (OSPM) for negotiating processor P and T state changes for power limiting. PMBus-compliant power supplies provide the capability to monitoring input power consumption, which is necessary to support NM.

4.7.1.1 Hardware Requirements

NM is supported only on platforms that have the NM FW functionality loaded and enabled on the Management Engine (ME) in the SSB and that have a BMC present to support the external LAN interface to the ME. NM power limiting features requires a means for the ME to monitor input power consumption for the platform. This capability is generally provided by means of PMBus-compliant power supplies although an alternative model using a simpler SMBus power monitoring device is possible (there is potential loss in accuracy and responsiveness using non-PMBus devices). The NM SmaRT/CLST feature does specifically require PMBus-compliant power supplies as well as additional hardware on the baseboard.

4.7.1.2 Features

NM provides feature support for policy management, monitoring and querying, alerts and notifications, and an external interface protocol. The policy management features implement specific IT goals that can be specified as policy directives for NM. Monitoring and querying features enable tracking of power consumption. Alerts and notifications provide the foundation for automation of power management in the data center management stack. The external interface specifies the protocols that must be supported in this version of NM.

4.7.1.3 ME Firmware Update

On server platforms, the ME FW uses a single operational image with a limited-functionality recovery image. In order to upgrade an operational image, a boot to recovery image must be performed. Unlike last generation platforms, the ME FW does not support an IPMI update mechanism except for the case that the system is configured with a dual-ME (redundant) image. In order to conserve flash space, which the ME FW shares with BIOS, EPSD systems only support a single ME image. For this case, ME update is only supported by means of BIOS performing a direct update of the flash component. The recovery image only provides the basic functionality that is required to perform the update; therefore other ME FW features are not functional therefore when the update is in progress.

4.7.1.4 SmaRT/CLST

The power supply optimization provided by SmaRT/CLST relies on a platform HW capability as well as ME FW support. When a PMBus-compliant power supply detects insufficient input voltage, an overcurrent condition, or an over-temperature condition, it will assert the SMBAlert# signal on the power supply SMBus (a.k.a. the PMBus). Through the use of external gates, this results in a momentary assertion of the PROCHOT# and MEMHOT# signals to the processors, thereby throttling the processors and memory. The ME FW also sees the SMBAlert# assertion, queries the power supplies to determine the condition causing the assertion, and applies an algorithm to either release or prolong the throttling, based on the situation.

System power control modes include:

1. SmaRT: Low AC input voltage event; results in a onetime momentary throttle for each event to the maximum throttle state
2. Electrical Protection CLST: High output energy event; results in a throttling hiccup mode with fixed maximum throttle time and a fix throttle release ramp time.
3. Thermal Protection CLST: High power supply thermal event; results in a throttling hiccup mode with fixed maximum throttle time and a fix throttle release ramp time.

When the SMBAlert# signal is asserted, the fans will be gated by HW for a short period (~100ms) to reduce overall power consumption. It is expected that the interruption to the fans will be of short enough duration to avoid false lower threshold crossings for the fan tach sensors; however, this may need to be comprehended by the fan monitoring FW if it does have this side-effect.

ME FW will log an event into the SEL to indicate when the system has been throttled by the SmaRT/CLST power management feature. This is dependent on ME FW support for this sensor. Please refer ME FW EPS for SEL log details.

4.7.1.4.1 Dependencies on PMBus-compliant Power Supply Support

The SmaRT/CLST system feature depends on functionality present in the ME NM SKU. This feature requires power supplies that are compliant with the *PMBus Specification,* Revision 1.2.

4.8 EU Lot 6 Mode

The European Union has set forth a stringent standby power consumption target for systems that are used as primary computing devices in office environments. Owing to the fact in office environments, pedestal servers are being used more and more as workstations and that Value servers could make their way into Home servers, this solution is being requested for some pedestal servers. HW support for EU Lot6 will only be available for specific EPSD pedestal products.

In order to meet the standby power requirements for EU Lot6 it is necessary to remove power to the BMC, along with other components, when in the S5 state. As this operational mode impacts system feature support, the user has the option of enabling and disabling this mode from the BIOS setup screen utility.

BIOS is responsible for enabling/disabling the system hardware for EU Lot6 operation. It notifies the BMC of the current state with the OEM command Set EULot6 Mode. The BMC saves the state in persistent store and uses it to control special EU Lot6 internal processing during boot, sensor monitoring, and so on as needed.

Wake-on-LAN (WOL) is not supported in EU Lot6 mode.

4.8.1.1 Impact to System Features

The following system features are lost or impacted when EU Lot6 mode is enabled:

- Increased boot time (~15-20s) when system is DC power cycled.
    - This is due to the fact that both the BMC and BIOS are booting at the same time when the system is powered on (to S0 state). BIOS will need to allow extra time for the BMC to initialize to the point where it can communicate with BIOS.

    Note: Even when EU Lot6 is not enabled and the system is AC cycled, this increased boot time is applicable if a user immediately attempts to power the system up (for example, pressing the power button), as in this case both the BMC and BIOS are booting at the same time.
- No LAN manageability when on standby, and therefore no remote OOB power on by BMC.
- No support for SOL or KVM for monitoring the entire boot process.
    - Since BMC is initializing at the same time as BIOS, it will not be possible to have an SOL or KVM session established from the beginning of the system boot.
- FP status LED will behave differently (it will be off when on standby) rather than showing fault conditions present at the time the system was powered down.
- No beep code due to uninstalled CPU.
- No monitoring of any sensors when on standby.
- No detection/logging of any ThermTrip faults.
    - These result as the system is shut down by HW so BMC will not be available to detect that they occurred.
- Sensor monitoring after DC power-on will be delayed by the time it takes BMC to initialize its sensor subsystem (~15 to 20s), possibly losing SEL events or failing to provide correct FP LED status LED indication.

    Note: This delay occurs on each AC cycle even when EU Lot6 mode is disabled.
- Chassis intrusion not detected when in standby

5. System Security

5.1 BIOS Password Protection

The BIOS uses passwords to prevent unauthorized tampering with the server setup. Passwords can restrict entry to the BIOS Setup, restrict use of the Boot Popup menu, and suppress automatic USB device reordering.
There is also an option to require a Power On password entry in order to boot the system. If the Power On Password function is enabled in Setup, the BIOS will halt early in POST to request a password before continuing POST.

Both Administrator and User passwords are supported by the BIOS. An Administrator password must be installed in order to set the User password. The maximum length of a password is 14 characters. A password can have alphanumeric (a-z, A-Z, 0-9) characters and it is case sensitive. Certain special characters are also allowed, from the following set:

! @ # $ % ^ & * ( ) - _ + = ?

The Administrator and User passwords must be different from each other. An error message will be displayed if there is an attempt to enter the same password for one as for the other.
The use of “Strong Passwords” is encouraged, but not required. In order to meet the criteria for a “Strong Password”, the password entered must be at least 8 characters in length, and must include at least one each of alphabetic, numeric, and special characters. If a “weak” password is entered, a popup warning message will be displayed, although the weak password will be accepted.

Once set, a password can be cleared by changing it to a null string. This requires the Administrator password, and must be done through BIOS Setup or other explicit means of changing the passwords. Clearing the Administrator password will also clear the User password.

Alternatively, the passwords can be cleared by using the Password Clear jumper if necessary. Resetting the BIOS configuration settings to default values (by any method) has no effect on the Administrator and User passwords.

Entering the User password allows the user to modify only the System Time and System Date in the Setup Main screen. Other setup fields can be modified only if the Administrator password has been entered. If any password is set, a password is required to enter the BIOS setup.

The Administrator has control over all fields in the BIOS setup, including the ability to clear the User password and the Administrator password.

It is strongly recommended that at least an Administrator Password be set, since not having set a password gives everyone who boots the system the equivalent of Administrative access. Unless an Administrator password is installed, any User can go into Setup and change BIOS settings at will.

In addition to restricting access to most Setup fields to viewing only when a User password is entered, defining a User password imposes restrictions on booting the system. In order to simply boot in the defined boot order, no password is required. However, the F6 Boot popup prompts for a password, and can only be used with the Administrator password. Also, when a

User password is defined, it suppresses the USB Reordering that occurs, if enabled, when a new USB boot device is attached to the system. A User is restricted from booting in anything other than the Boot Order defined in the Setup by an Administrator.
As a security measure, if a User or Administrator enters an incorrect password three times in a row during the boot sequence, the system is placed into a halt state. A system reset is required to exit out of the halt state. This feature makes it more difficult to guess or break a password.

In addition, on the next successful reboot, the Error Manager displays a Major Error code 0048, which also logs a SEL event to alert the authorized user or administrator that a password access failure has occurred.

5.2 Trusted Platform Module (TPM) Support

The Trusted Platform Module (TPM) option is a hardware-based security device that addresses the growing concern on boot process integrity and offers better data protection. TPM protects the system start-up process by ensuring it is tamper-free before releasing system control to the operating system. A TPM device provides secured storage to store data, such as security keys and passwords. In addition, a TPM device has encryption and hash functions. The server board implements TPM as per TPM PC Client Specifications revision 1.2 by the Trusted Computing Group (TCG).

A TPM device is optionally installed onto a high density 14-pin connector labeled “TPM” on the server board, and is secured from external software attacks and physical theft. A pre-boot environment, such as the BIOS and operating system loader, uses the TPM to collect and store unique measurements from multiple factors within the boot process to create a system fingerprint. This unique fingerprint remains the same unless the pre-boot environment is tampered with. Therefore, it is used to compare to future measurements to verify the integrity of the boot process.

After the system BIOS completes the measurement of its boot process, it hands off control to the operating system loader and in turn to the operating system. If the operating system is TPMenabled, it compares the BIOS TPM measurements to those of previous boots to make sure the
system was not tampered with before continuing the operating system boot process. Once the operating system is in operation, it optionally uses TPM to provide additional system and data security (for example, Microsoft Vista* supports Bitlocker drive encryption).

5.2.1 TPM security BIOS

The BIOS TPM support conforms to the *TPM PC Client Implementation Specification* for Conventional BIOS and to the *TPM Interface Specification,* and the *Microsoft Windows BitLocker* Requirements*. The role of the BIOS for TPM security includes the following:

- Measures and stores the boot process in the TPM microcontroller to allow a TPM enabled operating system to verify system boot integrity.
- Produces EFI and legacy interfaces to a TPM-enabled operating system for using TPM.
- Produces ACPI TPM device and methods to allow a TPM-enabled operating system to send TPM administrative command requests to the BIOS.

- Verifies operator physical presence. Confirms and executes operating system TPM administrative command requests.
- Provides BIOS Setup options to change TPM security states and to clear TPM ownership.

For additional details, refer to the *TCG PC Client Specific Implementation Specification*, the *TCG PC Client Specific Physical Presence Interface Specification*, and the *Microsoft BitLocker* Requirement* documents.

5.2.2 Physical Presence

Administrative operations to the TPM require TPM ownership or physical presence indication by the operator to confirm the execution of administrative operations. The BIOS implements the operator presence indication by verifying the setup Administrator password.

A TPM administrative sequence invoked from the operating system proceeds as follows:

1. User makes a TPM administrative request through the operating system's security software.
2. The operating system requests the BIOS to execute the TPM administrative command through TPM ACPI methods and then resets the system.
3. The BIOS verifies the physical presence and confirms the command with the operator.
4. The BIOS executes TPM administrative command(s), inhibits BIOS Setup entry and boots directly to the operating system which requested the TPM command(s).

5.2.3 TPM Security Setup Options

The BIOS TPM Setup allows the operator to view the current TPM state and to carry out rudimentary TPM administrative operations. Performing TPM administrative options through the BIOS setup requires TPM physical presence verification.

Using BIOS TPM Setup, the operator can turn ON or OFF TPM functionality and clear the TPM ownership contents. After the requested TPM BIOS Setup operation is carried out, the option reverts to No Operation.

The BIOS TPM Setup also displays the current state of the TPM, whether TPM is enabled or disabled and activated or deactivated. Note that while using TPM, a TPM-enabled operating system or application may change the TPM state independent of the BIOS setup. When an operating system modifies the TPM state, the BIOS Setup displays the updated TPM state.

The BIOS Setup TPM Clear option allows the operator to clear the TPM ownership key and allows the operator to take control of the system with TPM. You use this option to clear security settings for a newly initialized system or to clear a system for which the TPM ownership security key was lost.

5.2.3.1 Security Screen

To enter the BIOS Setup, press the F2 function key during boot time when the OEM or Intel logo displays. The following message displays on the diagnostics screen and under the Quiet Boot

logo screen:
Press <F2> to enter setup

When the Setup is entered, the Main screen displays. The BIOS Setup utility provides the Security screen to enable and set the user and administrative passwords and to lock out the front panel buttons so they cannot be used. The Intel® Server Board S5520URT provides TPM settings through the security screen.

To access this screen from the Main screen, select the **Security** option.

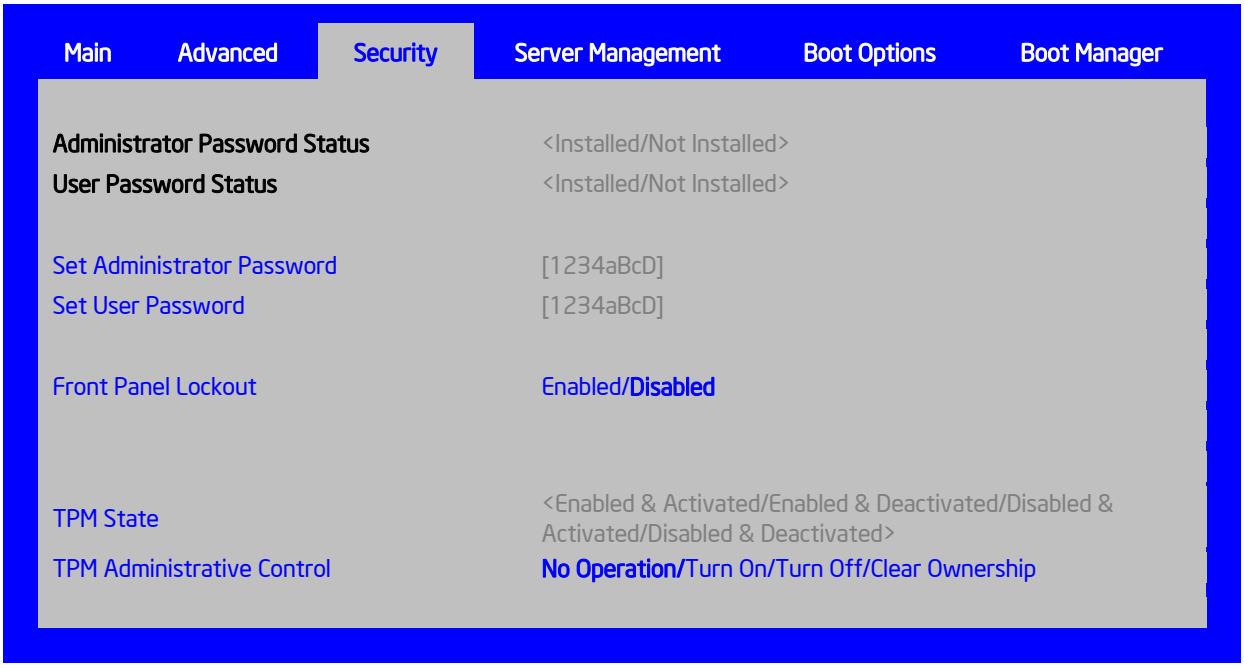


Figure 26. Setup Utility – TPM Configuration Screen

Table 29. TSetup Utility – Security Configuration Screen Fields

Setup Item	Options	Help Text	Comments
TPM State*	Enabled and Activated Enabled and Deactivated Disabled and Activated Disabled and Deactivated		**Information only**. Shows the current TPM device state. A disabled TPM device will not execute commands that use TPM functions and TPM security operations will not be available. An enabled and deactivated TPM is in the same state as a disabled TPM except setting of TPM ownership is allowed if not present already. An enabled and activated TPM executes all commands that use TPM functions and TPM security operations will be available.
TPM Administrative Control**	**No Operation** Turn On Turn Off Clear Ownership	[No Operation] - No changes to current state. [Turn On] - Enables and activates TPM. [Turn Off] - Disables and deactivates TPM. [Clear Ownership] - Removes the TPM ownership authentication and returns the TPM to a factory default state. **Note**: The BIOS setting returns to [No Operation] on every boot cycle by default.	

5.3 Intel® Trusted Execution Technology

The Intel® Xeon® Processor E5-4600/2600/2400/1600 Product Families support Intel® Trusted Execution Technology (Intel® TXT), which is a robust security environment. Designed to help protect against software-based attacks, Intel® Trusted Execution Technology integrates new security features and capabilities into the processor, chipset and other platform components. When used in conjunction with Intel® Virtualization Technology, Intel® Trusted Execution Technology provides hardware-rooted trust for your virtual applications.
This hardware-rooted security provides a general-purpose, safer computing environment capable of running a wide variety of operating systems and applications to increase the confidentiality and integrity of sensitive information without compromising the usability of the platform.

Intel® Trusted Execution Technology requires a computer system with Intel® Virtualization Technology enabled (both VT-x and VT-d), an Intel® Trusted Execution Technology-enabled processor, chipset and BIOS, Authenticated Code Modules, and an Intel® Trusted Execution

Technology compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel® Trusted Execution Technology requires the system to include a TPM v1.2, as defined by the Trusted Computing Group TPM PC Client specifications, Revision 1.2.

When available, Intel Trusted Execution Technology can be enabled or disabled in the processor by a BIOS Setup option.

For general information about Intel® TXT, visit the Intel® Trusted Execution Technology website, http://www.intel.com/technology/security/.

6. Connector/Header Locations and Pin-outs

6.1 Power Connectors

6.1.1 Main Power Connector

Main server board power is supplied by one 12-pin power connector. The connector is labeled as “MAIN PWR” on the left bottom of the server board. The following tables provide the pin-out for “MAIN PWR” connector.

Table 30. Main Power Connector Pin-out

Pin	Signal name	Pin	Signal name
1	P3V3	13	P3V3
2	P3V3	14	N12V
3	GND	15	GND
4	P5V	16	FM_PS_EN_PSU_N
5	GND	17	GND
6	P5V	18	GND
7	GND	19	GND
8	PWRGD_PS_PWROK_PSU_R1	20	NC_PS_RES_TP
9	P5V_STBY_PSU	21	P5V
10	P12V	22	P5V
11	P12V	23	P5V
12	P3V3	24	GND

6.1.2 CPU Power Connectors

On the server board are two white 8-pin CPU power connectors labeled “CPU_1 PWR” and “CPU_2 PWR”. The following table provides the pin-out for both connectors.

Table 31. CPU_1 Power Connector Pin-out

Pin	Signal name	Pin	Signal name
1	GND	5	P12V1
2	GND	6	P12V1
3	GND	7	P12V3A
4	GND	8	P12V3A

Table 32. CPU_2 Power Connector Pin-out

Pin	Signal name	Pin	Signal name
1	GND	5	P12V2
2	GND	6	P12V2
3	GND	7	P12V3B
4	GND	8	P12V3B

6.2 Front Panel Header and Connectors

The server board includes several connectors that provide various possible front panel options. This section provides a functional description and pin-out for each connector.

6.2.1 Front Panel Header

Included on the left edge of the server board is a 30-pin header consists of a 24-pin SSI compatible front panel header and a 4-pin header to support optional NIC3/4 LEDs. The 24-pin SSI front panel header provides various front panel features including:

- Power/Sleep Button
- System ID Button
- NMI Button
- NIC Activity LEDs
- Hard Drive Activity LEDs
- System Status LED
- System ID LED

The following table provides the pin-out for this 30-pin header.

Table 33. Front Panel Header Pin-out

Pin	Signal name	Pin	Signal name
1	P3V3_AUX	2	P3V3_AUX
3	Key	4	P5V_STBY
5	FP_PWR_LED_BUF_N	6	FP_ID_LED_BUF_N
7	P3V3	8	FP_LED_STATUS_GREEN_BUF_N
9	LED_HDD_ACTIVITY_N	10	FP_LED_STATUS_AMBER_BUF_N
11	FP_PWR_BTN_N	12	LED_NIC_LINK0_ACT_BUF_N
13	GND	14	LED_NIC_LINK0_LNKUP_BUF_N
15	FP_RST_BTN_N	16	SMB_SENSOR_3V3STBY_DATA
17	GND	18	SMB_SENSOR_3V3STBY_CLK
19	FP_ID_BTN_N	20	FP_CHASSIS_INTRUSION
21	PU_FM_SIO_TEMP_SENSOR	22	LED_NIC_LINK1_ACT_BUF_N
23	FP_NMI_BTN_N	24	LED_NIC_LINK1_LNKUP_BUF_N
25	<Empty Pin>	26	<Empty Pin>
27	LED_NIC_LINK2_ACT_FP_N	28	LED_NIC_LINK3_ACT_FP_N
29	LED_NIC_LINK2_LNKUP_FP_N	30	LED_NIC_LINK3_LNKUP_FP_N

6.2.2 Front Panel USB Connector

The server board includes a 10-pin connector, that when cabled, can provide up to two USB ports to a front panel. The following table provides the connector pin-out.

Table 34. Front Panel USB Connector Pin-out

Pin	Signal Name	Pin	Signal Name
1	P5V_USB_FP	2	P5V_USB_FP
3	USB2_P13_F_DN	4	USB2_P11_F_DN
5	USB2_P13_F_DP	6	USB2_P11_F_DP
7	GND	8	GND
9	KEY	10	NA

6.2.3 Local Control Panel Connector

The server board includes a 7-pin connector that is used when the system is configured with the Intel Local Control Panel with LCD support. The following table provides the pin-out for this connector.

Table 35. Local Front Panel Connector Pin-out

Pin	Signal Name	Pin	Signal Name
1	SMB_SENSOR_3V3STBY_DATA	2	GND
3	SMB_SENSOR_3V3STBY_CLK	4	P3V3_AUX
5	FM_LCP_ENTER_N	6	FM_LCP_LEFT_N
7	FM_LCP_RIGHT_N		

6.3 On Board Storage Connectors

The server board provides connectors for support of several storage device options. This section provides a functional overview and pin-out of each connector.

6.3.1 SATA Connectors: 6Gbps

The board includes two white single port SATA only connectors capable of transfer rates of up to 6Gb/s. The following table provides the pin-out for both connectors.

Table 36. SATA 6Gbps Connector Pin-out

Pin	Signal Name
1	GND
2	SATA_TX_P
3	SATA_TX_N
4	GND
5	SATA_RX_N
6	SATA_RX_P
7	GND

6.3.2 Multiport Mini-SAS/SATA Connectors

The board includes two 40-pin high density multiport mini-SAS/SATA connectors. On the board, these connectors are labeled as “SCU0 port(0-3)” supporting the chipset embedded SCU0 controller, and “SCU1 Port(4-7)”, supporting the embedded SCU1 controller. Both connectors can support up to four SATA or SAS ports each. By default, only the connector labeled “SCU0 Port(0-3)” is enabled and has support for up to four SATA ports capable. The connector labeled “SCU1 Port(4-7)” is only enabled when an optional 8-port SAS or SATA Intel® RAID C600 Upgrade Key is installed. The following tables provide the pin-out for each connector.

Table 37. Multiport SAS/SATA Connector Pin-out ("SCU_0 (0-3)")

Pin	Signal name	Pin	Signal name
A1	GROUND	B1	GROUND
A2	SAS0_RX_C_DP	B2	SAS0_TX_C_DP
A3	SAS0_RX_C_DN	B3	SAS0_TX_C_DN
A4	GROUND	B4	GROUND
A5	SAS1_RX_C_DP	B5	SAS1_TX_C_DP
A6	SAS1_RX_C_DN	B6	SAS1_TX_C_DN
A7	GROUND	B7	GROUND
A8	TP_SAS1_BACKPLANE_TYPE	B8	SGPIO_SAS1_CLOCK
A9	GROUND	B9	SGPIO_SAS1_LOAD
A10	SGPIO_SAS1_DATAOUT	B10	GROUND
A11	SGPIO_SAS1_DATAIN	B11	PD_SAS1_CONTROLLER_TYPE
A12	GROUND	B12	GROUND
A13	SAS2_RX_C_DP	B13	SAS2_TX_C_DP
A14	SAS2_RX_C_DN	B14	SAS2_TX_C_DN
A15	GROUND	B15	GROUND
A16	SAS3_RX_C_DP	B16	SAS3_TX_C_DP
A17	SAS3_RX_C_DN	B17	SAS3_TX_C_DN
A18	GROUND	B18	GROUND
MTH1	GROUND	MTH5	GROUND
MTH2	GROUND	MTH6	GROUND
MTH3	GROUND	MTH7	GROUND
MTH4	GROUND	MTH8	GROUND

Table 38. Multiport SAS/SATA Connector Pin-out ("SCU_1 (4-7)")

Pin	Signal name	Pin	Signal name
A1	GROUND	B1	GROUND
A2	SAS4_RX_C_DP	B2	SAS4_TX_C_DP
A3	SAS4_RX_C_DN	B3	SAS4_TX_C_DN
A4	GROUND	B4	GROUND
A5	SAS5_RX_C_DP	B5	SAS5_TX_C_DP
A6	SAS5_RX_C_DN	B6	SAS5_TX_C_DN
A7	GROUND	B7	GROUND
A8	TP_SAS2_BACKPLANE_TYPE	B8	SGPIO_SAS2_CLOCK
A9	GROUND	B9	SGPIO_SAS2_LOAD
A10	SGPIO_SAS2_DATAOUT	B10	GROUND
A11	SGPIO_SAS2_DATAIN	B11	PD_SAS2_CONTROLLER_TYPE
A12	GROUND	B12	GROUND
A13	SAS6_RX_C_DP	B13	SAS6_TX_C_DP
A14	SAS6_RX_C_DN	B14	SAS6_TX_C_DN
A15	GROUND	B15	GROUND
A16	SAS7_RX_C_DP	B16	SAS7_TX_C_DP
A17	SAS7_RX_C_DN	B17	SAS7_TX_C_DN
A18	GROUND	B18	GROUND
MTH1	GROUND	MTH5	GROUND
MTH2	GROUND	MTH6	GROUND
MTH3	GROUND	MTH7	GROUND
MTH4	GROUND	MTH8	GROUND

6.3.3 Intel® RAID C600 Upgrade Key Connector

The server board provides one connector to support Intel® RAID C600 Upgrade Key. The Intel® RAID C600 Upgrade Key is a small PCB board that enables different versions of RAID 5 software stack and/or upgrade from SATA to SAS storage functionality. The pin configuration of connector is identical and defined in the following table.

Table 39. Intel® RAID C600 Upgrade Key Connector Pin-out

Pin	Signal Name
1	GND
2	FM_PBG_DYN_SKU_KEY
3	GND
4	FM_SSB_SAS_SATA_RAID_KEY

6.3.4 HSBP_I2C Header

Table 40. HSBP_I2C Header Pin-out

Pin	Signal Name
1	SMB_HSBP_3V3STBY_DATA
2	GND
3	SMB_HSBP_3V3STBY_CLK

6.3.5 HDD LED Header

The server board includes a 2-pin hard drive activity LED header used with some SAS/SATA controller add-in cards. The header has the following pin-out.

Table 41. HDD LED Header Pin-out

Pin	Signal Name	Pin	Signal Name
1	LED_HDD_ACT_N	2	NA

6.3.6 Internal Type- A USB Connector

The server board includes two internal Type-A USB connector. The following table provides the pin-out for this connector.

Table 42. Type-A USB Connector Pin-out

Pin	Signal Name	Pin	Signal Name
1	P5V	2	USB2_P2_F_DN
3	USB2_P2_F_DP	4	GND

6.3.7 Internal eUSB SSD Header

The server board includes one 10-pin internal eUSB header with an intended usage of supporting USB SSD devices. The following table provides the pin-out for this connector.

Table 43. eUSB SSD Header Pin-out

Pin	Signal Name	Pin	Signal Name
1	5V	2	NC
3	USB2_P0_DN	4	NC
5	USB2_P0_DP	6	NC
7	GND	8	NC
9	Key	10	LED_HDD_ACT_ZEPHER_N

6.4 Management and Security Connectors

6.4.1 RMM4_Lite Connector

A 7-pin Intel® RMM4 Lite connector is included on the server board to support the optional Intel® Remote Management Module 4. There is no support for third-party management cards on this server board.

Table 44. RMM4_Lite Connector Pin-out

Pin	Signal Name	Pin	Signal Name
1	P3V3_AUX	2	DI
3	KEY	4	CLK
5	DO	6	GND
7	CS_N	8	GND

6.4.2 RMM4_NIC Connector

Table 45. RMM4_NIC Connector Pin-out

Pin	Signal Name	Pin	Signal Name
1	3V3_AUX	2	MDIO
3	3V3_AUX	4	MDC
5	GND	6	TXD_0
7	GND	8	TXD_1
9	GND	10	TXD_2
11	GND	12	TXD_3
13	GND	14	TX_CTL
15	GND	16	RX_CTL
17	GND	18	RXD_0
19	GND	20	RXD_1
21	GND	22	RXD_2
23	GND	24	RXD_3
25	GND	26	TX_CLK
27	GND	28	RX_CLK
29	GND	30	PRESENT#

6.4.3 TPM Connector

Table 46. TPM Connector Pin-out

Pin	Signal Name	Pin	Signal Name
1	Key	2	LPC_LAD<1>
3	LPC_LAD<0>	4	GND
5	IRQ_SERIAL	6	LPC_FRAME_N
7	P3V3	8	GND
9	RST_IBMC_NIC_N_R2	10	CLK_33M_TPM
11	LPC_LAD<3>	12	GND
13	GND	14	LPC_LAD<2>

6.4.4 PMBUS Connector

Table 47. PMBUS Connector Pin-out

Pin	Signal name
1	SMB_PMBUS_CLK_R
2	SMB_PMBUS_DATA_R
3	IRQ_SML1_PMBUS_ALERT_RC_N
4	GND
5	P3V3

6.4.5 Chassis Intrusion Header

The server board includes a 2-pin chassis intrusion header which can be used when the chassis is configured with a chassis intrusion switch. The header has the following pin-out.

Table 48. Chassis Intrusion Header Pin-out

Header State	Description
Pins 1 and 2 closed	FM_INTRUDER_HDR_N is pulled HIGH. Chassis cover is closed.
Pins 1 and 2 open	FM_INTRUDER_HDR_N is pulled LOW. Chassis cover is removed.

6.4.6 IPMB Connector

Table 49. IPMB Connector Pin-out

Pin	Signal Name
1	SMB_IPMB_5VSTBY_DATA
2	GND
3	SMB_IPMB_5VSTBY_CLK
4	P5V_STBY

6.5 FAN Connectors

The server board provides support for nine fans. Seven of them are system cooling fans, two of them are CPU fans.

6.5.1 System FAN Connectors

The six system cooling fan connectors near the front edge of the board are 6-Pin connectors; the one system cooling fan near edge of the board is a 4-Pin connectors. Following table provides the pin-out for all system fan connectors.

Table 50. 6-pin System FAN Connector Pin-out

Pin	Signal Name
1	GND
2	12V
3	TACH
4	PWM
5	PRSNT
6	FAULT

Table 51. 4-pin System FAN Connector Pin-out

Pin	Signal Name
1	GND
2	12V
3	TACH
4	PWM

6.5.2 CPU FAN Connector

The two CPU fan connectors are 4-pin fan connectors. Following table provides the pin-out for CPU fan connectors.

Table 52. CPU FAN Connector Pin-out

Pin	Signal Name
1	GND
2	12V
3	TACH
4	PWM

6.6 Serial Port and Video Connectors

The server board includes two serial port connectors.

6.6.1 Serial Port A Connector (DB9, for Intel® Server Board S2600IP only)

Serial-A is an external RJ45 type connector and has the following pin-out configuration.

Table 53. Serial Port A Connector Pin-out

Pin	Signal Name	Pin	Signal Name
1	SPA_DCD	2	SPA_SIN
3	SPA_SOUT_N	4	SPA_DTR
5	GND	6	SPA_DSR
7	SPA_RTS	8	SPA_CTS
9	SPA_RI		

6.6.2 Serial Port B Connector

Serial-B is an internal 10-pin DH-10 connector and has the following pin-out.

Table 54. Serial Port B Connector Pin-out

Pin	Signal Name	Pin	Signal Name
1	SPA_DCD	2	SPA_DSR
3	SPA_SIN	4	SPA_RTS
5	SPA_SOUT_N	6	SPA_CTS
7	SPA_DTR	8	SPA_RI
9	GND		

6.6.3 Video Connector (For Intel® Server Board S2600IP only)

The following table details the pin-out definition of the external VGA connector.

Table 55. Video Connector Pin-out details

Pin	Signal Name
1	CRT_RED
2	CRT_GREEN
3	CRT_BLUE
4	N/C
5	GND
6	GND
7	GND
8	GND
9	P5V
10	GND
11	NC
12	CRT_DDCDATA
13	CRT_HSYNC
14	CRT_VSYNC
15	CRT_DDCCLK

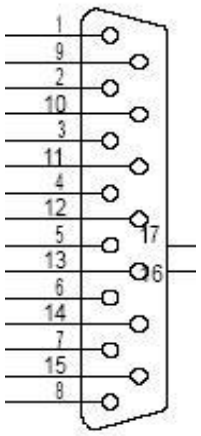


Figure 27. Video Connector Pin-out

6.6.4 Internal Video header (For Intel® Workstation Board W2600CR only)

Pin	Signal Name
1	CRT_RED
2	GND
3	CRT_Green
4	GND
5	CRT_Blue
6	GND
7	CRT_VSYNC
8	GND
9	CRT_HSYN
10	Key
11	CRT_DDCDATA
12	VIDEO_IN_USE signal
13	CRT_DDCCLK
14	5V

Note: Intel® Corporation server boards support peripheral components and can contain a number of high-density VLSI and power delivery components that need adequate airflow to cool. Intel's own chassis are designed and tested to meet the intended thermal requirements of these components when the fully integrated system is used together. It is the responsibility of the system integrator that chooses not to use Intel® developed server building blocks to consult vendor datasheets and operating parameters to determine the amount of airflow required for their specific application and environmental conditions. Intel Corporation cannot be held responsible if components fail or the server board does not operate correctly when used outside any of its published operating or non-operating limits.

7. Jumper Blocks

The server boards have several 3-pin jumper blocks that you can use to configure, protect, or recover specific features of the server boards.

The following symbol identifies Pin 1 on each jumper block on the silkscreen: ▼

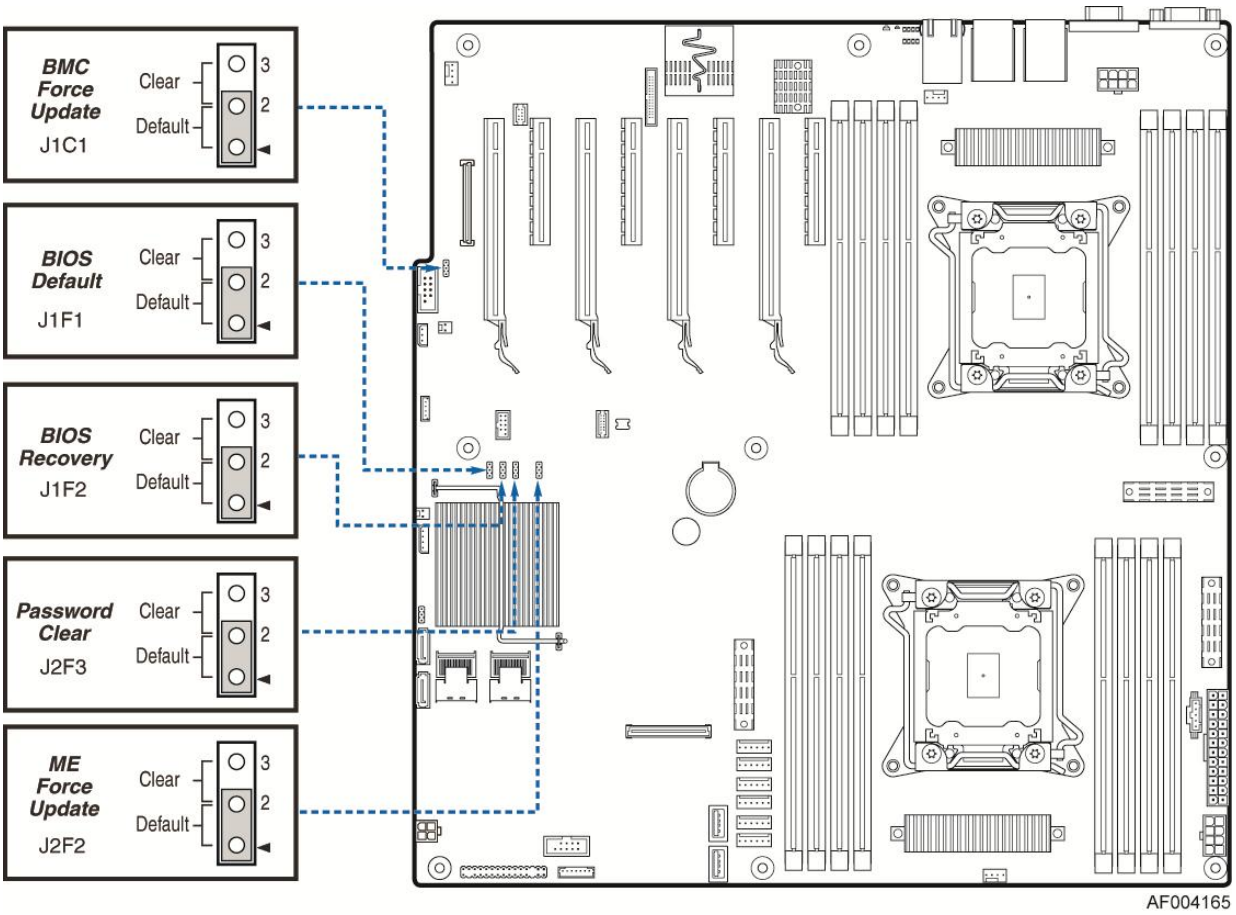


Figure 28. Jumper Blocks (J1C3, J1F1, J1F2, J2F3, J2F2)

Table 56. Server Board Jumpers (J1C3, J1F1, J1F2, J2F3, J2F2)

Jumper Name	Pins	System Results
J1F2: BIOS Recovery	1-2	Pins 1-2 should be connected for normal system operation. **(Default)**
	2-3	The main system BIOS does not boot with pins 2-3 connected. The system only boots from EFI-bootable recovery media with a recovery BIOS image present.
J1F1: Bios Default (CMOS Clear)	1-2	These pins should have a jumper in place for normal system operation. **(Default)**
	2-3	If pins 2-3 are connected when AC power unplugged, the CMOS settings clear in 5 seconds. Pins 2-3 should not be connected for normal system operation.
J2F2: ME Force	1-2	ME Firmware Force Update Mode – Disabled **(Default)**

Jumper Name	Pins	System Results
Update	2-3	ME Firmware Force Update Mode – Enabled
J1C1: BMC Force Update	1-2	BMC Firmware Force Update Mode – Disabled **(Default)**
	2-3	BMC Firmware Force Update Mode – Enabled
J2F3: Password Clear	1-2	These pins should have a jumper in place for normal system operation. **(Default)**
	2-3	To clear administrator and user passwords, power on the system with pins 2-3 connected. The administrator and user passwords clear in 5-10 seconds after power on. Pins 2-3 should not be connected for normal system operation.

7.1 BIOS Default and Password Reset Usage Procedure

The BIOS Default (CMOS Clear) and Password Reset recovery features are designed to achieve the desired operation with minimum system down time. The usage procedure for these two features has changed from previous generation Intel® boards. The following procedure outlines the new usage model.

7.1.1 Set BIOS to default (Clearing the CMOS)

1. Power down the server and unplug the AC power cord.
2. Open the server chassis. For instructions, see your server chassis documentation.
3. Move the jumper from the default operating position (covering pins 1 and 2) to the reset/clear position (covering pins 2 and 3).
4. Wait five seconds.
5. Move the jumper back to the default position, covering pins 1 and 2.
6. Close the server chassis and reconnect the AC power cord.
7. Power up the server.

The CMOS is now cleared and you can reset it by going into the BIOS setup.

Note: Removing AC power before performing the CMOS clear operation causes the system to automatically power up and immediately power down, after the procedure is followed and AC power is re-applied. If this happens, remove the AC power cord again, wait 30 seconds, and reinstall the AC power cord. Power up the system and proceed to the <F2> BIOS Setup utility to reset the preferred settings.

7.1.2 Clearing the Password

1. Power down the server. Do not unplug the power cord.
2. Open the chassis. For instructions, see your server chassis documentation.
3. Move the jumper from the default operating position (covering pins 1 and 2) to the password clear position (covering pins 2 and 3).
4. Close the server chassis.
5. Power up the server and then press <F2> to enter the BIOS menu to check if the password is cleared.

6. Power down the server.
7. Open the chassis and move the jumper back to its default position (covering pins 1 and 2).
8. Close the server chassis.
9. Power up the server.

The password is now cleared and you can reset it by going into the BIOS setup.

7.2 Force BMC Update Procedure

When performing a standard BMC firmware update procedure, the update utility places the BMC into an update mode, allowing the firmware to load safely onto the flash device. In the unlikely event the BMC firmware update process fails due to the BMC not being in the proper update state, the server boards provide a Force BMC Update jumper that forces the BMC into the proper update state. In the event the standard BMC firmware update process fails, complete the following procedure:

1. Power down and remove the AC power cord.
2. Open the server chassis. See your server chassis documentation for instructions.
3. Move the jumper from the default operating position (covering pins 1 and 2) to the enabled position (covering pins 2 and 3).
4. Close the server chassis.
5. Reconnect the AC power cord and power up the server.
6. Perform the BMC firmware update procedure as documented in the BMC firmware update package. After successful completion of the firmware update process, the firmware update utility may generate an error stating the BMC is still in update mode.
7. Power down and remove the AC power cord.
8. Open the server chassis.
9. Move the jumper from the enabled position (covering pins 2 and 3) to the disabled position (covering pins 1 and 2).
10. Close the server chassis.
11. Reconnect the AC power cord and power up the server.

Note: When the Force BMC Update jumper is set to the enabled position, normal BMC functionality is disabled. You should never run the server with the Force BMC Update jumper set in this position. You should only use this jumper setting when the standard firmware update process fails. When the server is running normally, this jumper must remain in the default/disabled position.

7.3 BIOS Recovery Jumper

The following procedure boots the recovery BIOS and flashes the normal BIOS:

1. Turn off the system power.
2. Move the BIOS recovery jumper to the recovery state.

3. Insert a bootable BIOS recovery media containing the new BIOS image files.

4. Turn on the system power.

The BIOS POST screen will appear displaying the progress, and the system will boot to the EFI shell. The EFI shell then executes the Startup.nsh batch file to start the flash update process. The user should then switch off the power and return the recovery jumper to its normal position. The user should not interrupt the BIOS POST on the first boot after recovery.

When the flash update completes:

1. Remove the recovery media.

2. Turn off the system power.

3. Restore the jumper to its original position.

4. Turn on the system power.

5. Re-flash any custom blocks, such as user binary or language blocks.

The system should now boot using the updated system BIOS.

7.4 ME Force Update Jumper

When performing the standard ME force update procedure, the update utility places the ME into an update mode, allowing the ME to load safely onto the flash device. In the unlikely event ME firmware update process fails due to ME not being in the proper update state, the server board provides an Integrated BMC Force Update jumper, which forces the ME into the proper update state. The following procedure should be completed in the event the standard ME firmware update process fails.

1. Power down and remove the AC power cord.

2. Open the server chassis. For instructions, see your server chassis documentation.

3. Move jumper from the default operating position (covering pins 1 and 2) to the enabled position (covering pins 2 and 3).

4. Close the server chassis.

5. Reconnect the AC cord and power up the server.

6. Perform the ME firmware update procedure as documented in the README.TXT file that is included in the given ME firmware update package (same package as BIOS).

7. Power down and remove the AC power cord.

8. Open the server chassis.

9. Move jumper from the enabled position (covering pins 2 and 3) to the disabled position (covering pins 1 and 2).

10. Close the server chassis.
11. Reconnect the AC cord and power up the server.

8. Intel® Light Guided Diagnostics

Both server boards have several onboard diagnostic LEDs to assist in troubleshooting board-level issues. This section provides a description of the location and function of each LED on the server boards.

8.1 5-volt Stand-by LED

Several server management features of these server boards require a 5-V stand-by voltage supplied from the power supply. The features and components that require this voltage must be present when the system is “power-down”. The LED is illuminated when AC power is applied to the platform and 5-V stand-by voltage is supplied to the server board by the power supply.

8.2 Fan Fault LED

Fan fault LEDs are present for the two CPU fans and the one rear system fan. The fan fault LEDs illuminate when the corresponding fan has fault.

8.3 CPU Fault LED

CPU fault LED should correspond to the socket with the failed or disabled CPU. The CPU LEDs illuminate when CPU failure or Disable.

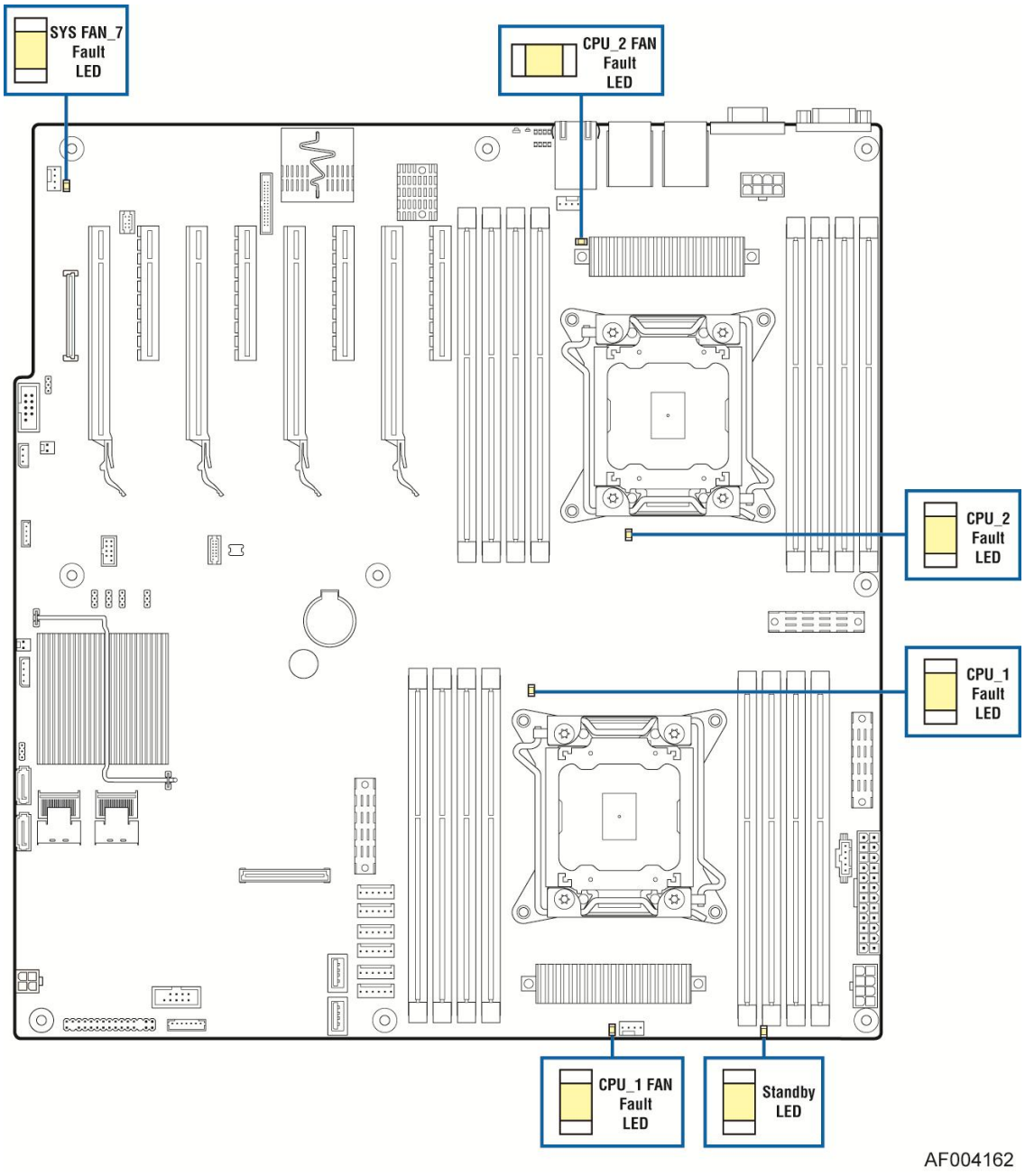


Figure 29. Stand by LED, Fan Fault LED and CPU Fault LED Location

8.4 DIMM Fault LEDs

The server board provide memory fault LED for each DIMM socket. These LEDs are located as shown in the following figure. The DIMM fault LED illuminates when the corresponding DIMM slot has memory installed and a memory error occurs.

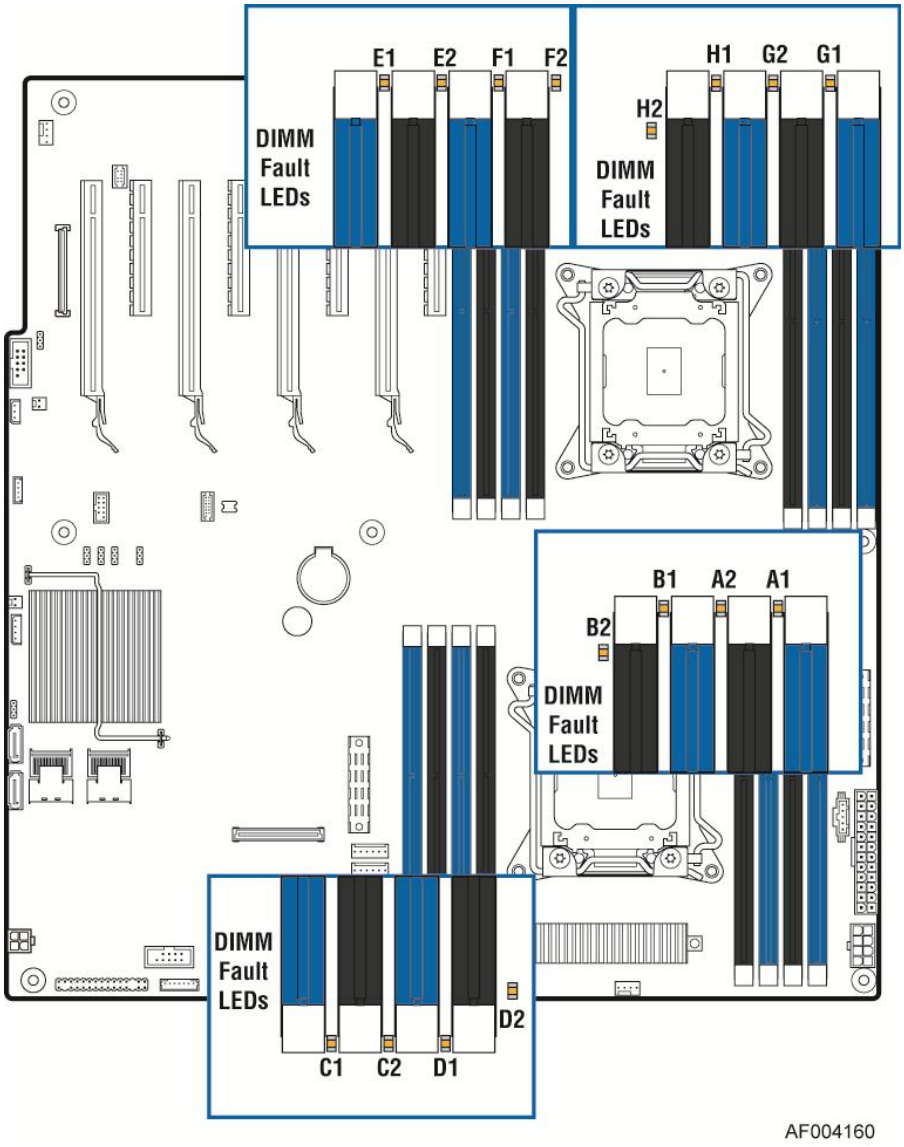


Figure 30. DIMM Fault LED's Location

8.5 System ID LED, System Status LED and POST Code Diagnostic LEDs

The server boards provide LEDs for system ID, system status and POST code. These LEDs are located in the rear I/O area of the server board as shown in the following figure.

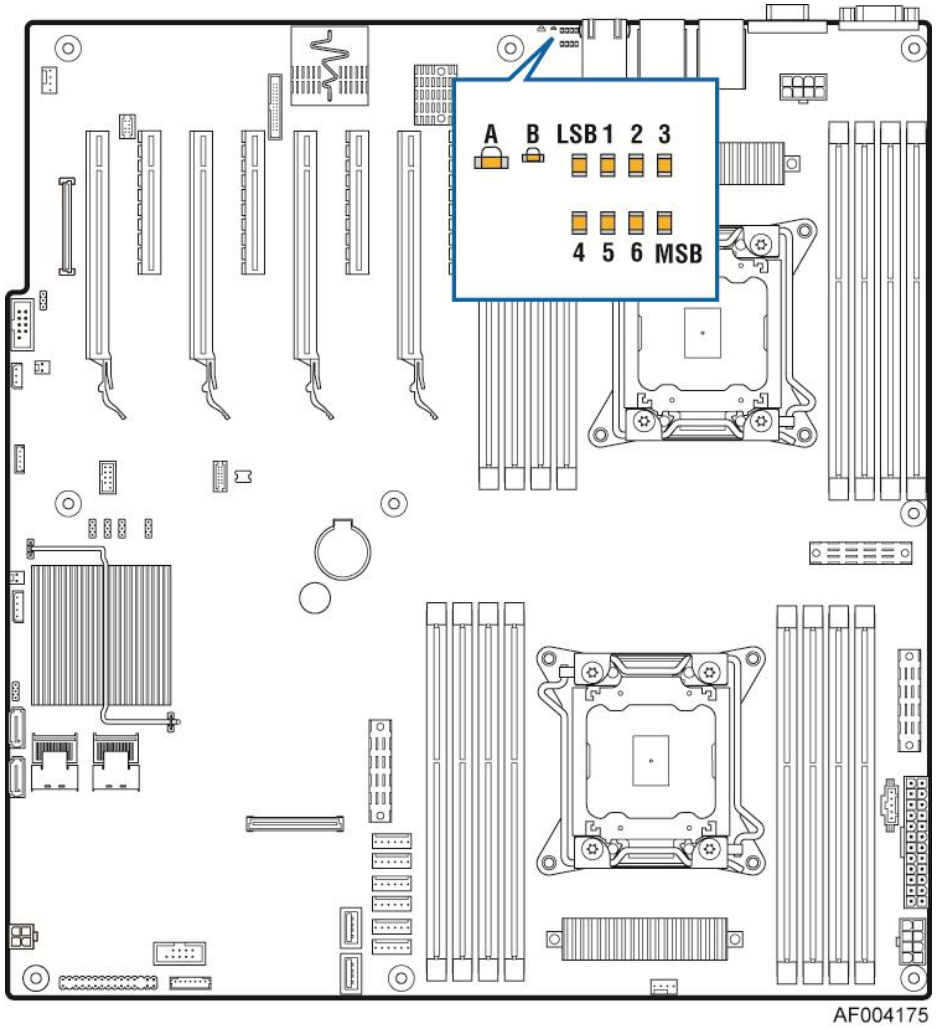


Figure 31. Location of System Status, System ID and POST Code Diagnostic LEDs

LED Name	Description
A	System Status LED
B	System ID LED
LSB 1 2 3 4 5 6 MSB	Post Code Diagnostic LEDs

8.5.1 System ID LED

You can illuminate the blue System ID LED using either of the following two mechanisms:

- By pressing the System ID Button on the system front control panel, the ID LED displays a solid blue color until the button is pressed again.
- By issuing the appropriate hex IPMI “Chassis Identify” value, the ID LED will either blink blue for 15 seconds and turn off or will blink indefinitely until the appropriate hex IPMI Chassis Identify value is issue to turn it off.

8.5.2 System Status LED

The bi-color (green/amber) System Status LED operates as follows:

Table 57. System Status LED

Color	State	Criticality	Description
Green	Solid on	Ok	Indicates that the System Status is 'Healthy'. The system is not exhibiting any errors. AC power is present and BMC has booted and manageability functionality is up and running.
Green	~1 Hz blink	Degraded	System degraded: 1. Redundancy loss such as power-supply or fan. Applies only if the associated platform sub-system has redundancy capabilities. 2. Fan warning or failure when the number of fully operational fans is more than minimum number needed to cool the system. 3. Non-critical threshold crossed – Temperature (including HSBP temp), voltage, input power to power supply, output current for main power rail from power supply and Processor Thermal Control (Therm Ctrl) sensors. 4. Power supply predictive failure occurred while redundant power supply configuration was present. 5. Unable to use all of the installed memory (more than 1 DIMM installed). 6. Correctable Errors over a threshold and migrating to a spare DIMM (memory sparing). This indicates that the user no longer has spared DIMMs indicating a redundancy lost condition. Corresponding DIMM LED lit. 7. In mirrored configuration, when memory mirroring takes place and system loses memory redundancy. 8. Battery failure. 9. BMC executing in uBoot. (Indicated by Chassis ID blinking at Blinking at 3Hz). System in degraded state (no manageability). BMC uBoot is running but has not transferred control to BMC Linux. Server will be in this state 6-8 seconds after BMC reset while it pulls the Linux image into flash 10. BMC booting Linux. (Indicated by Chassis ID solid ON). System in degraded state (no manageability). Control has been passed from BMC uBoot to BMC Linux itself. It will be in this state for ~10-~20 seconds. 11. BMC Watchdog has reset the BMC. 12. Power Unit sensor offset for configuration error is asserted. 13. HDD HSC is off-line or degraded.
Amber	~1 Hz blink	Non-critical	Non-fatal alarm – system is likely to fail: 1. Critical threshold crossed – Voltage, temperature (including HSBP temp), input power to power supply, output current for main power rail from power supply and PROCHOT (Therm Ctrl) sensors. 2. VRD Hot asserted. 3. Minimum number of fans to cool the system not present or failed 4. Hard drive fault 5. Power Unit Redundancy sensor – Insufficient resources offset (indicates not enough power supplies present). 6. In non-sparing and non-mirroring mode if the threshold of correctable errors is crossed within the window

Color	State	Criticality	Description
Amber	Solid on	Critical, non-recoverable	Fatal alarm – system has failed or shutdown: 1. CPU CATERR signal asserted. 2. MSID mismatch detected (CATERR also asserts for this case). 3. CPU 1 is missing. 4. CPU ThermalTrip. 5. No power good – power fault. 6. DIMM failure when there is only 1 DIMM present and hence no good memory present. 7. Runtime memory uncorrectable error in non-redundant mode 1. 8. DIMM Thermal Trip or equivalent. 9. SSB Thermal Trip or equivalent. 10. CPU ERR2 signal asserted. 11. BMC/Video memory test failed. (Chassis ID shows blue/solid-on for this condition). 12. Both uBoot BMC FW images are bad. (Chassis ID shows blue/solid on for this condition). 13. 13. 240VA fault
Off	N/A	Not ready	AC power off

8.5.3 POST Code Diagnostic LEDs

During the system boot process, the BIOS executes a number of platform configuration processes, each of which is assigned a specific hex POST code number. As each configuration routine is started, the BIOS displays the given POST code to the POST code diagnostic LED's on the back edge of the server boards. To assist in troubleshooting a system hang during the POST process, you can use the diagnostic LEDs to identify the last POST process executed.

Table 58. POST Code Diagnostic LEDs

A. Diagnostic LED #7 (MSB LED)	E. Diagnostic LED #3
B. Diagnostic LED #6	F. Diagnostic LED #2
C. Diagnostic LED #5	G. Diagnostic LED #1
D. Diagnostic LED #4	H. Diagnostic LED #0 (LSB LED)

9. Design and Environmental Specifications

9.1 Products Design Specifications

Operation of the Intel® Server Board S2600IP and Workstation Board W2600CR at conditions beyond those shown in the following table may cause permanent damage to the system. Exposure to absolute maximum rating conditions for extended periods may affect system reliability.

Table 59. Server Board Design Specifications

Operating Temperature	0º C to 55º C[1] (32º F to 131º F)
Non-Operating Temperature	-40º C to 70º C (-40º F to 158º F)
DC Voltage	± 5% of all nominal voltages
Shock (Unpackaged)	Trapezoidal, 35 G, 135 inches/sec
Shock (Packaged) < 20 pounds 20 to < 40 pounds 40 to < 80 pounds 80 to < 100 pounds 100 to < 120 pounds 120 pounds	 36 inches 30 inches 24 inches 18 inches 12 inches 9 inches
Vibration (Unpackaged)	5 Hz to 500 Hz 3.13 g RMS random

Note:

[1] Chassis design must provide proper airflow to avoid exceeding the processor maximum case temperature.

Disclaimer Note: Intel Corporation server boards contain a number of high-density VLSI and power delivery components that need adequate airflow to cool. Intel ensures through its own chassis development and testing that when Intel® server building blocks are used together, the fully integrated system will meet the intended thermal requirements of these components. It is the responsibility of the system integrator who chooses not to use Intel® developed server building blocks to consult vendor datasheets and operating parameters to determine the amount of airflow required for their specific application and environmental conditions. Intel Corporation cannot be held responsible, if components fail or the server board does not operate correctly when used outside any of its published operating or non-operating limits.

9.2 MTBF

The following is the calculated Mean Time Between Failures (MTBF) 30° C (ambient air). These values are derived using a historical failure rate and multiplied by factors for application, electrical and/or thermal stress and for device maturity. You should view MTBF estimates as “reference numbers” only.

- Calculation Model: Telcordia Issue 2, method I case 3
- Operating Temperature: Server in 30° C ambient air
- Operating Environment: Ground Benign, Controlled
- Duty Cycle: 100%

- Quality Level: II

Table 60. Intel® Server Board S2600IP MTBF Estimate

Assembly Name	Failure Rate	MTBF
Mother Board	4,981.828605	200,730
Integrated Circuits	888.017556	1,126,104
Transistor_Bipolar	142.288706	7,027,965
Transistor_MOSFET	394.540757	2,534,592
Diodes	24.364143	41,043,923
Diodes_LED	30.002406	33,330,661
Resistors	1,134.467959	881,470
Capacitors	379.972284	2,631,771
Cap, Al Elect	741.486991	1,348,641
Inductors	148.990773	6,711,825
Connections	1,213.354514	824,161
Misc	94.901757	10,537,213

Table 61. Intel® Workstation Board W2600CR MTBF Estimate

Assembly Name	Failure Rate	MTBF
Mother Board	5,247.668190	190,561
Integrated Circuits	951.031471	1,051,490
Transistor_Bipolar	147.372000	6,785,549
Transistor_MOSFET	404.110588	2,474,570
Diodes	36.808324	27,167,768
Diodes_LED	30.002406	33,330,661
Resistors	1,204.023273	830,549
Capacitors	413.065171	2,420,925
Cap, Al Elect	770.924084	1,297,145
Inductors	175.282101	5,705,089
Connections	1,216.849949	821,794
Misc	127.585507	7,837,881

9.3 Server Board Power Requirements

This section provides power supply design guidelines for a system using the Intel® Server Board S2600IP and Workstation Board W2600CR including voltage and current specifications, and power supply on/off sequencing characteristics. The following diagram shows the power distribution implemented on these server boards.

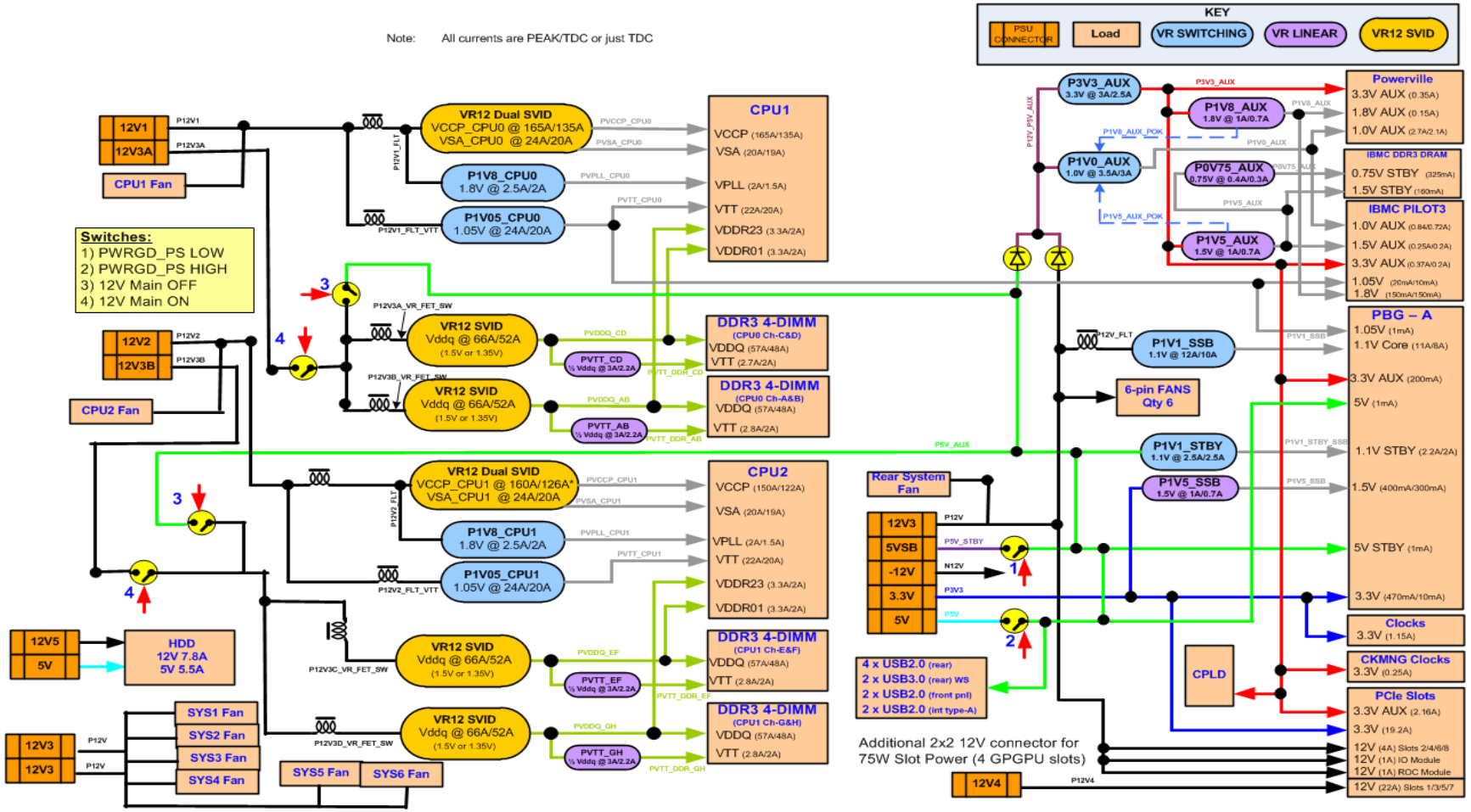


Figure 32. Power Distribution Block Diagram

9.3.1 Processor Power Support

The server boards support the Thermal Design Power (TDP) guideline for Intel® Xeon® processors. The Flexible Motherboard Guidelines (FMB) is followed to determine the suggested thermal and current design values for anticipating future processor needs. The following table provides maximum values for DTS, TDP power and T_{CASE} for the compatible Intel® E5-2600 processor family series.

Table 62. Intel® Xeon® Processor Dual Processor TDP profile

Max TDP Power	Max Tcase (°C)	Max DTS (°C)
130W	85°C	104.4 for 6 core
		100 for 8 core
150W	67°C	84.8

9.4 Power Supply Output Requirements

This section is for reference purposes only. The intent is to provide guidance to system designers to determine a power supply to use with these server boards. This section specifies the power supply requirements Intel used to develop a power supply for its server system.

9.4.1 Output Power/Currents

The following tables define the minimum power and current ratings. The power supply must meet both static and dynamic voltage regulation requirements for all conditions.

Table 63. Minimum Load Ratings

Parameter	Min	Max.	Peak	Unit
3.3V	0.5	18.0		A
5V	0.3	15.0		A
12V1	0.7	24.0	28.0	A
12V2	0.7	24.0	28.0	A
12V3	1.5	18.0		A
– 12V	0.0	0.5		A
5Vstby	0.0	3.0	3.5	A

Notes:

1. Combined continuous power for all output shall not exceed 550W.
2. Peak combined power for all outputs shall not exceed 630W for 20 seconds.
3. Max combined power of 12V1, 12V2, and 12V3 shall not exceed 530W.
4. Max combined power on 3.3V and 5V shall not exceed 120W.

9.4.2 Cross Loading

The power supply shall maintain voltage regulation limit when operated over the following cross loading conditions.

Table 64. Loading Conditions

	3.3V	5V	12V1	12V2	12V3	-12V	5Vstby	Total Power	12V Power	3.3V/5V Power
Load1	18	12.1	12	12	11.7	0	0.3	550	428	120
Load2	13.5	15	12	12	11.2	0.5	0.3	549	422	120
Load3	2.5	2	20	20	4.2	0	0.3	550	530	18
Load4	2.5	2	13.1	13.1	18	0	0.3	550	530	18
Load5	0.5	0.3	15	15	6.5	0.5	3	462	438	3
Load6	16	4	1	1	3.5	0	0.3	140	66	73
Load7	16	13	1	1	9	0.5	3	271	132	118

9.4.3 Standby Output

The 5VSB output shall be present when an AC input greater than the power supply turn on voltage is applied.

9.4.4 Voltage Regulation

The power supply output voltages must stay within the following voltage limits when operating at steady state and dynamic loading conditions. These limits include the peak-peak ripple/noise. These shall be measured at the output connectors.

Table 65.Voltage Regulation Limits

Parameter	Tolerance	Min	Nom	Max	Units
+3.3V	- 3%/+5%	+3.20	+3.30	+3.46	V_{rms}
+5V	- 4%/+5%	+4.80	+5.00	+5.25	V_{rms}
+12V1	- 4%/+5%	+11.52	+12.00	+12.60	V_{rms}
+12V2	- 4%/+5%	+11.52	+12.00	+12.60	V_{rms}
+12V3	- 4%/+5%	+11.52	+12.00	+12.60	V_{rms}
- 12V	- 10%/+10%	- 13.20	-12.00	-10.80	V_{rms}
+5VSB	- 4%/+5%	+4.80	+5.00	+5.25	V_{rms}

9.4.5 Dynamic Loading

The output voltages shall remain within limits specified for the step loading and capacitive loading specified in the table below. The load transient repetition rate shall be tested between 50Hz and 5kHz at duty cycles ranging from 10%-90%. The load transient repetition rate is only a test specification. The Δ step load may occur anywhere within the MIN load to the MAX load conditions.

Table 66. Transient Load Requirements

Output	Δ Step Load Size (See note 2)	Load Slew Rate	Test capacitive Load
+3.3V	6.0A	0.5 A/μsec	970 μF
+5V	4.0A	0.5 A/μsec	400 μF
12V1+12V2+12V3	23A	0.5 A/μsec	2200 μF [1,2]
+5VSB	0.5A	0.5 A/μsec	20 μF

Notes:

1. Step loads on each 12V output may happen simultaneously.
2. The +12V should be tested with 2200µF evenly split between the four +12V rails
3. This will be tested over the range of load conditions in section 9.4.2

9.4.6 Capacitive Loading

The power supply shall be stable and meet all requirements with the following capacitive loading ranges.

Table 67. Capacitive Loading Conditions

Output	Min	Max	Units
+3.3V	250	5000	µF
+5V	400	5000	µF
+12V	500	8000	µF
-12V	1	350	µF
+5VSB	20	350	µF

9.4.7 Grounding

The output ground of the pins of the power supply provides the output power return path. The output connector ground pins shall be connected to the safety ground (power supply enclosure). This grounding should be well designed to ensure passing the max allowed Common Mode Noise levels.

The power supply shall be provided with a reliable protective earth ground. All secondary circuits shall be connected to protective earth ground. Resistance of the ground returns to chassis shall not exceed 1.0 mΩ. This path may be used to carry DC current.

9.4.8 Closed loop stability

The power supply shall be unconditionally stable under all line/load/transient load conditions including capacitive load ranges specified in Section 4.6. A minimum of **45 degrees phase margin** and -**10dB-gain margin** is required. The power supply manufacturer shall provide proof of the unit's closed-loop stability with local sensing through the submission of Bode plots. Closed-loop stability must be ensured at the maximum and minimum loads as applicable.

9.4.9 Residual Voltage Immunity in Standby mode

The power supply should be immune to any residual voltage placed on its outputs (Typically a leakage voltage through the system from standby output) up to **500mV**. There shall be no additional heat generated, nor stressing of any internal components with this voltage applied to any individual or all outputs simultaneously. It also should not trip the protection circuits during turn on.
The residual voltage at the power supply outputs for no load condition shall not exceed **100mV** when AC voltage is applied and the PSON# signal is de-asserted.

9.4.10 Common Mode Noise

The Common Mode noise on any output shall not exceed **350mV pk-pk** over the frequency band of 10Hz to 20MHz. The measurement shall be made across a 100Ω resistor between each of DC outputs, including ground at the DC power connector and chassis ground (power

subsystem enclosure). The test set-up shall use a FET probe such as Tektronix model P6046 or equivalent.

9.4.11 Soft Starting

The Power Supply shall contain control circuit which provides monotonic soft start for its outputs without overstress of the AC line or any power supply components at any specified AC line or load conditions.

9.4.12 Zero Load Stability Requirements

When the power subsystem operates in a no load condition, it does not need to meet the output regulation specification, but it must operate without any tripping of over-voltage or other fault circuitry. When the power subsystem is subsequently loaded, it must begin to regulate and source current without fault.

9.4.13 Ripple/Noise

The maximum allowed ripple/noise output of the power supply is defined in the table below. This is measured over a bandwidth of 10Hz to 20MHz at the power supply output connectors. A 10μF tantalum capacitor in parallel with a 0.1μF ceramic capacitor is placed at the point of measurement.

Table 68. Ripples and Noise

+3.3V	+5V	+12V1,2,3	-12V	+5VSB
50mVp-p	50mVp-p	120mVp-p	200mVp-p	50mVp-p

The test set-up is shown below.

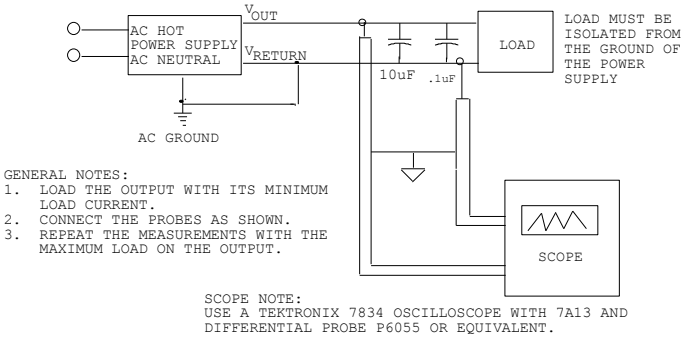


Figure 33. Differential Noise test setup

Note:
When performing this test, the probe clips and capacitors should be located close to the load.

9.4.14 Timing Requirements

These are the timing requirements for the power supply operation. The output voltages must rise from 10% to within regulation limits (T_{vout_rise}) within 2 to 50ms, except for 5VSB - it is allowed to rise from 1 to 25ms. The +3.3V, +5V and +12V1,+12V2 ,+12V3 output voltages

should start to rise approximately at the same time**. All outputs must rise monotonically**. Each output voltage shall reach regulation within 50ms (T_{vout_on}) of each other during turn on of the power supply. Each output voltage shall fall out of regulation within 400ms (T_{vout_off}) of each other during turn off. Table 69 shows the timing requirements for the power supply being turned on and off by the AC input, with PSON held low and the PSON signal, with the AC input applied. All timing requirements must be met for the cross loading condition in section TBD.

Table 69. Output Voltage Timing

Item	Description	Min	Max	Units
T_{vout_rise}	Output voltage rise time from each main output.	2	50	ms
	Output rise time for the 5Vstby output.	1	25	ms
T_{vout_on}	All main outputs must be within regulation of each other within this time.		50	ms
T_{vout_off}	All main outputs must leave regulation within this time.		400	ms

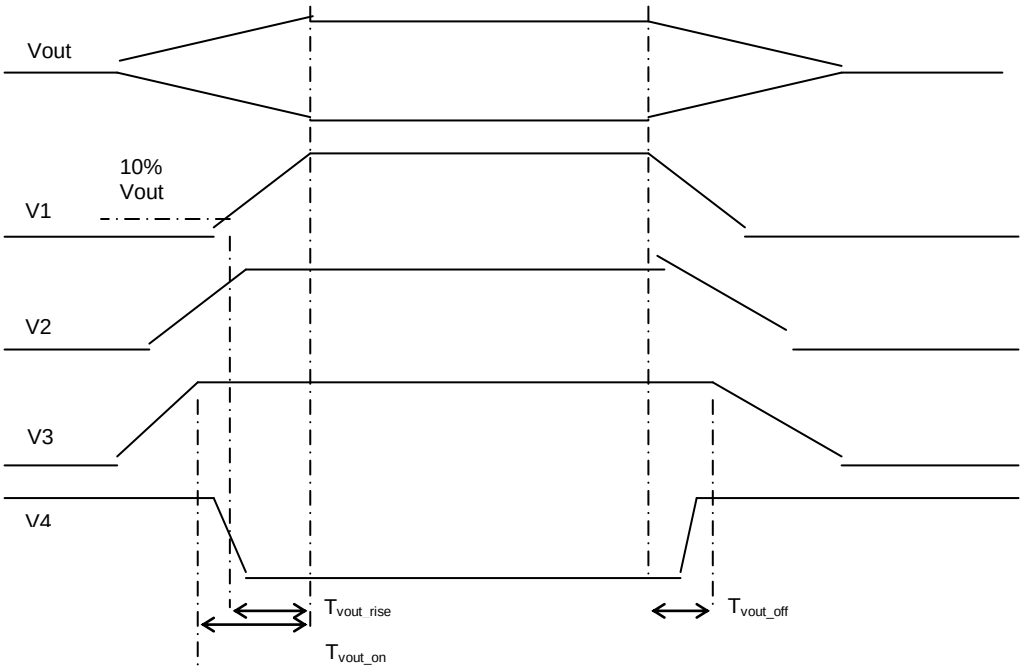


Figure 34. Output Voltage Timing

Table 70. Turn On/Off Timing

Item	Description	MIN	MAX	UNITS
$T_{sb\_on\_delay}$	Delay from AC being applied to 5VSB being within regulation.		1500	ms
$T_{ac\_on\_delay}$	Delay from AC being applied to all output voltages being within regulation.		2500	ms

Item	Description	MIN	MAX	UNITS
T_{vout_holdup}	Time all output voltages stay within regulation after loss of AC. Tested at 75% of maximum load.	13		ms
T_{pwok_holdup}	Delay from loss of AC to de-assertion of PWOK. Tested at 75% of maximum load.	12		ms
$T_{pson\_on\_delay}$	Delay from PSON# active to output voltages within regulation limits.	5	400	ms
T_{pson_pwok}	Delay from PSON# deactivate to PWOK being de-asserted.		50	ms
T_{pwok_on}	Delay from output voltages within regulation limits to PWOK asserted at turn on.	100	500	ms
T_{pwok_off}	Delay from PWOK de-asserted to output voltages (3.3V, 5V, 12V, -12V) dropping out of regulation limits.	1		ms
T_{pwok_low}	Duration of PWOK being in the de-asserted state during an off/on cycle using AC or the PSON signal.	100		ms
T_{sb_vout}	Delay from 5VSB being in regulation to O/Ps being in regulation at AC turn on.	10	1000	ms
T_{5VSB_holdup}	Time the 5VSB output voltage stays within regulation after loss of AC.	70		ms

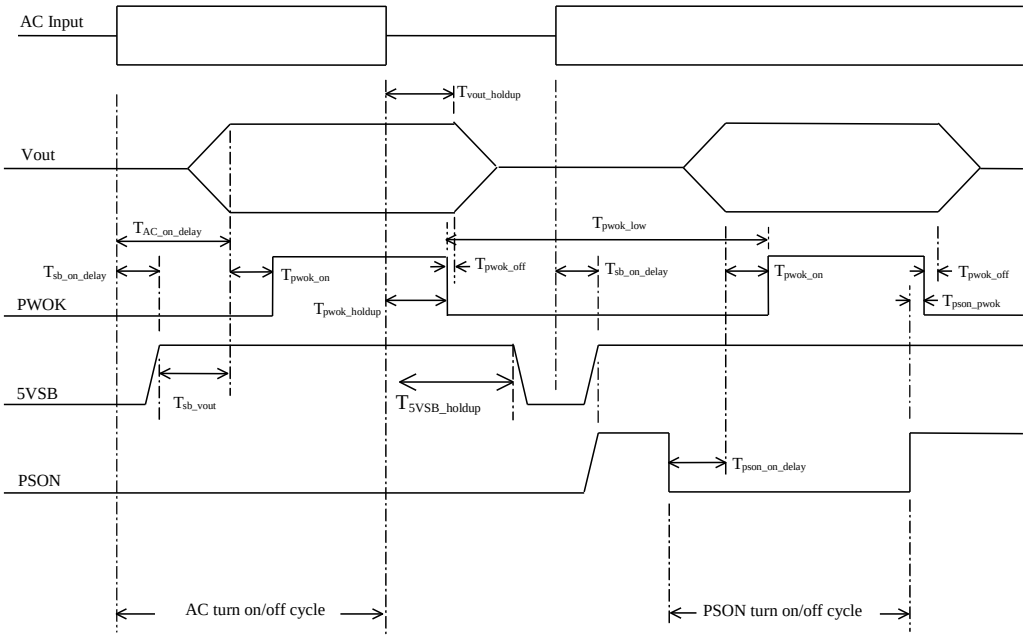


Figure 35. Turn On/Off Timing (Power Supply Signals)

Appendix A: Integration and Usage Tips

- When adding or removing components or peripherals from the server board, AC power must be removed. With AC power plugged into the server board, 5-V standby is still present even though the server board is powered off.
- This server board supports The Intel® Xeon® Processor E5-2600 product family with a Thermal Design Power (TDP) of up to and including 135 Watts. Previous generations of Intel® Xeon® processors are not supported.
- Processors must be installed in order. CPU 1 must be populated for operating the server board.
- On the back edge of the server board are eight diagnostic LEDs that display a sequence of amber POST codes during the boot process. If the server board hangs during POST, LEDs display the last POST event run before the hang.
- This server board only supports registered DDR3 DIMMs (RDIMMs) and unbuffered DDR3 DIMMs (UDIMMs). Mixing of RDIMMs and UDIMMs is not supported.
- For the best performance, the number of DDR3 DIMMs installed should be balanced across both processor sockets and memory channels. For example, a two-DIMM configuration performs better than a one-DIMM configuration. In a two-DIMM configuration, DIMMs should be installed in DIMM sockets A1 and D1.
- The Intel® Remote Management Module 4 (Intel® RMM4) connector is not compatible with any previous versions of the Intel® Remote Management Module (Product Order Code – AXXRMM, AXXRMM2, and AXXRMM3).
- Clear the CMOS with AC power cord plugged. Removing the AC power before performing the CMOS clear operation causes the system to automatically power up and immediately power down after the CMOS clear procedure is followed and AC power is re-applied. If this happens, remove the AC power cord, wait 30 seconds, and then reconnect the AC power cord. Power up the system and proceed to the <F2> BIOS Setup utility to reset the desired settings.
- Normal Integrated BMC functionality is disabled with the BMC Force Update jumper set to the “enabled” position (pins 2-3). The server should never be run with the BMC Force Update jumper set in this position and should only be used when the standard firmware update process fails. This jumper should remain in the default (disabled) position (pins 1-2) when the server is running normally.
- When performing a normal BIOS update procedure, the BIOS recovery jumper must be set to its default position (pins 1-2).

Appendix B: BMC Sensor Tables

This appendix lists the sensor identification numbers and information about the sensor type, name, supported thresholds, assertion and de-assertion information, and a brief description of the sensor purpose. See the *Intelligent Platform Management Interface Specification, Version 2.0* for sensor and event/reading-type table information.

Sensor Type Codes

Sensor table given below lists the sensor identification numbers and information regarding the sensor type, name, supported thresholds, assertion and de-assertion information, and a brief description of the sensor purpose. Refer to the *Intelligent Platform Management Interface Specification, Version 2.0* for sensor and event/reading-type table information.

- **Sensor Type**
  The sensor type references the values in the Sensor Type Codes table in the Intelligent Platform Management Interface Specification Second Generation v2.0. It provides a context to interpret the sensor.
- **Event/Reading Type**
  The event/reading type references values from the Event/Reading Type Code Ranges and the Generic Event/Reading Type Code tables in the Intelligent Platform Management Interface Specification Second Generation v2.0. Digital sensors are specific type of discrete sensors that only have two states.
- **Event Thresholds/Triggers**
  The following event thresholds are supported for threshold type sensors:
  - [u,l][nr,c,nc] upper non-recoverable, upper critical, upper non-critical, lower non-recoverable, lower critical, lower non-critical uc, lc upper critical, lower critical

  Event triggers are supported event-generating offsets for discrete type sensors. The offsets can be found in the *Generic Event/Reading Type Code* or *Sensor Type Code* tables in the *Intelligent Platform Management Interface Specification Second Generation v2.0*, depending on whether the sensor event/reading type is generic or a sensor-specific response.
- **Assertion/Deassertion**
  Assertion and de-assertion indicators reveal the type of events this sensor generates:
  - As: Assertion
  - De: De-assertion
- **Readable Value/Offsets**
  - Readable value indicates the type of value returned for threshold and other non-discrete type sensors.
  - Readable offsets indicate the offsets for discrete sensors that are readable by means of the *Get Sensor Reading* command. Unless otherwise indicated, event triggers are readable. Readable offsets consist of the reading type offsets that do not generate events.
- **Event Data**
  Event data is the data that is included in an event message generated by the associated sensor. For threshold-based sensors, these abbreviations are used:
  - R: Reading value

  - T: Threshold value

- **Rearm Sensors**
  The rearm is a request for the event status for a sensor to be rechecked and updated upon a transition between good and bad states. Rearming the sensors can be done manually or automatically. This column indicates the type supported by the sensor. The following abbreviations are used in the comment column to describe a sensor:
  - A: Auto-rearm
  - M: Manual rearm
  - I: Rearm by init agent
- **Default Hysteresis**
  The hysteresis setting applies to all thresholds of the sensor. This column provides the count of hysteresis for the sensor, which can be 1 or 2 (positive or negative hysteresis).
- **Criticality**
  Criticality is a classification of the severity and nature of the condition. It also controls the behavior of the front panel status LED.
- **Standby**
  Some sensors operate on standby power. These sensors may be accessed and/or generate events when the main (system) power is off, but AC power is present.

Note: All sensors listed below may not be present on all platforms. Please check platform EPS section for platform applicability and platform chassis section for chassis specific sensors. Redundancy sensors will be only present on systems with appropriate hardware to support redundancy (for instance, fan or power supply).

Table 71. Integrated BMC Core Sensors

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
Power Unit Status *(Pwr Unit Status)*	01h	All	Power Unit 09h	Sensor Specific 6Fh	00 - Power down	OK	As and De	–	Trig Offset	A	X
					02 - 240 VA power down	Fatal					
					04 - A/C lost	OK					
					05 - Soft power control failure	Fatal					
					06 - Power unit failure						
Power Unit Redundancy[1] *(Pwr Unit Redund)*	02h	Chassis-specific	Power Unit 09h	Generic 0Bh	00 - Fully Redundant	OK	As and De	–	Trig Offset	M	X
					01 - Redundancy lost	Degraded					
					02 - Redundancy degraded	Degraded					
					03 - Non-redundant: sufficient resources. Transition from full redundant state.	Degraded					
					04 – Non-redundant: sufficient resources. Transition from insufficient state.	Degraded					
					05 - Non-redundant: insufficient resources	Fatal					
					06 – Redundant: degraded from fully redundant state.	Degraded					

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
					07 – Redundant: Transition from non-redundant state.	Degraded					
IPMI Watchdog *(IPMI Watchdog)*	03h	All	Watchdog 2 23h	Sensor Specific 6Fh	00 - Timer expired, status only 01 - Hard reset 02 - Power down 03 - Power cycle 08 - Timer interrupt	OK	As	–	Trig Offset	A	X
Physical Security *(Physical Scrty)*	04h	Chassis Intrusion is chassis-specific	Physical Security 05h	Sensor Specific 6Fh	00 - Chassis intrusion 04 - LAN leash lost	Degarded OK	As and De	–	Trig Offset	A	X
FP Interrupt *(FP NMI Diag Int)*	05h	Chassis-specific	Critical Interrupt 13h	Sensor Specific 6Fh	00 - Front panel NMI/diagnostic interrupt	OK	As	–	Trig Offset	A	–
SMI Timeout *(SMI Timeout)*	06h	All	SMI Timeout F3h	Digital Discrete 03h	01 – State asserted	Fatal	As and De	–	Trig Offset	A	–
System Event Log *(System Event Log)*	07h	All	Event Logging Disabled 10h	Sensor Specific 6Fh	02 - Log area reset/cleared	OK	As	–	Trig Offset	A	X
System Event *(System Event)*	08h	All	System Event 12h	Sensor Specific 6Fh	02 - Undetermined system H/W failure 04 – PEF action	Fatal OK	As and De As	-	Trig Offset	A	X
Button Sensor *(Button)*	09h	All	Button/Switch 14h	Sensor Specific 6Fh	00 – Power Button 02 – Reset Button	OK	AS	_	Trig Offset	A	X

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
BMC Watchdog	0Ah	All	Mgmt System Health 28h	Digital Discrete 03h	01 – State Asserted	Degraded	As	–	Trig Offset	A	-
Voltage Regulator Watchdog (VR Watchdog)	0Bh	All	Voltage 02h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	M	X
Fan Redundancy[1] *(Fan Redundancy)*	0Ch	Chassis-specific	Fan 04h	Generic 0Bh	00 - Fully redundant	OK	As and De	–	Trig Offset	A	–
					01 - Redundancy lost	Degraded					
					02 - Redundancy degraded	Degraded					
					03 - Non-redundant: Sufficient resources. Transition from redundant	Degraded					
					04 - Non-redundant: Sufficient resources. Transition from insufficient.	Degraded					
					05 - Non-redundant: insufficient resources.	Non-Fatal					
					06 – Non-Redundant: degraded from fully redundant.	Degraded					
					07 - Redundant degraded from non-redundant	Degraded					
SSB Thermal Trip *(SSB Therm Trip)*	0Dh	All	Temperature 01h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	M	X
IO Module Presence (IO Mod Presence)	0Eh	Platform-specific	Module/Board 15h	Digital Discrete 08h	01 – Inserted/Present	OK	As and De	–	Trig Offset	M	-
SAS Module Presence (SAS Mod Presence)	0Fh	Platform-specific	Module/Board 15h	Digital Discrete 08h	01 – Inserted/Present	OK	As and De	–	Trig Offset	M	X

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
BMC Firmware Health (BMC FW Health)	10h	All	Mgmt Health 28h	Sensor Specific 6Fh	04 – Sensor Failure	Degraded	As	-	Trig Offset	A	X
System Airflow (System Airflow)	11h	All	Other Units 0Bh	Threshold 01h	–	–	–	Analog	–	–	–
FW Update Status	12h	All	Version Change 2Bh	OEM defined x70h	00h→Update started 01h→Update completed successfully. 02h→Update failure	OK	As	_	Trig Offset	A	_
IO Module2 Presence (IO Mod2 Presence)	13h	Platform-specific	Module/Board 15h	Digital Discrete 08h	01 – Inserted/Present	OK	As and De	–	Trig Offset	M	-
Baseboard Temperature 5 *(*Platform Specific*)*	14h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Baseboard Temperature 6 *(*Platform Specific*)*	15h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
IO Module2 Temperature (I/O Mod2 Temp)	16h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
PCI Riser 3 Temperature (PCI Riser 5 Temp)	17h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
PCI Riser 4 Temperature (PCI Riser 4 Temp)	18h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Baseboard +1.05V Processor3 Vccp *(BB +1.05Vccp P3)*	19h	Platform-specific	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
Baseboard +1.05V Processor4 Vccp *(BB +1.05Vccp P4)*	1Ah	Platform-specific	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard Temperature 1 *(*Platform Specific*)*	20h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Front Panel Temperature *(Front Panel Temp)*	21h	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
SSB Temperature *(SSB Temp)*	22h	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Baseboard Temperature 2 *(*Platform Specific*)*	23h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Baseboard Temperature 3 *(*Platform Specific*)*	24h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Baseboard Temperature 4 *(*Platform Specific*)*	25h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
IO Module Temperature (I/O Mod Temp)	26h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
PCI Riser 1 Temperature (PCI Riser 1 Temp)	27h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
IO Riser Temperature (IO Riser Temp)	28h	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
Hot-swap Backplane 1 Temperature (HSBP 1 Temp)	29h	Chassis-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Hot-swap Backplane 2 Temperature (HSBP 2 Temp)	2Ah	Chassis-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Hot-swap Backplane 3 Temperature (HSBP 3 Temp)	2Bh	Chassis-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
PCI Riser 2 Temperature (PCI Riser 2 Temp)	2Ch	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
SAS Module Temperature (SAS Mod Temp)	2Dh	Platform-specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Exit Air Temperature (Exit Air Temp)	2Eh	Chassis and Platform Specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Network Interface Controller Temperature (LAN NIC Temp)	2Fh	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Fan Tachometer Sensors (Chassis specific sensor names)	30h–3Fh	Chassis and Platform Specific	Fan 04h	Threshold 01h	[l] [c,nc]	nc = Degraded c = Non-fatal[2]	As and De	Analog	R, T	M	-
Fan Present Sensors *(Fan x Present)*	40h–4Fh	Chassis and Platform Specific	Fan 04h	Generic 08h	01 - Device inserted	OK	As and De	-	Triggered Offset	Auto	-
Power Supply 1 Status *(PS1 Status)*	50h	Chassis-specific	Power Supply	Sensor Specific	00 - Presence 01 - Failure	OK Degraded	As and	–	Trig Offset	A	X

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
			08h	6Fh	02 – Predictive Failure	Degraded	De				
					03 - A/C lost	Degraded					
					06 – Configuration error	OK					
Power Supply 2 Status *(PS2 Status)*	51h	Chassis-specific	Power Supply 08h	Sensor Specific 6Fh	00 - Presence	OK	As and De	–	Trig Offset	A	X
					01 - Failure	Degraded					
					02 – Predictive Failure	Degraded					
					03 - A/C lost	Degraded					
					06 – Configuration error	OK					
Power Supply 1 AC Power Input (PS1 Power In)	54h	Chassis-specific	Other Units 0Bh	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Power Supply 2 AC Power Input (PS2 Power In)	55h	Chassis-specific	Other Units 0Bh	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Power Supply 1 +12V % of Maximum Current Output (*PS1 Curr Out %*)	58h	Chassis-specific	Current 03h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Power Supply 2 +12V % of Maximum Current Output (*PS2 Curr Out %*)	59h	Chassis-specific	Current 03h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Power Supply 1 Temperature (*PS1 Temperature*)	5Ch	Chassis-specific	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Power Supply 2 Temperature (*PS2 Temperature*)	5Dh	Chassis-specific	Temperature	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Hard Disk Drive 16 - 24 Status (HDD 16 - 24 Status)	60h – 68h	Chassis-specific	Drive Slot 0Dh	Sensor Specific 6Fh	00 - Drive Presence	OK	As and De	–	Trig Offset	A	X
					01- Drive Fault	Degraded					

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
					07 - Rebuild/Remap in progress	Degraded					
	69h - 6Bh	Chassis-specific	Microcontroller 16h	Discrete 0Ah	04- transition to Off Line	Degraded		–	Trig Offset		X
Processor 1 Status *(P1 Status)*	70h	All	Processor 07h	Sensor Specific 6Fh	01 - Thermal trip	Fatal	As and De	–	Trig Offset	M	X
					07 - Presence	OK					
Processor 2 Status *(P2 Status)*	71h	All	Processor 07h	Sensor Specific 6Fh	01 - Thermal trip	Fatal	As and De	–	Trig Offset	M	X
					07 - Presence	OK					
Processor 3 Status *(P3 Status)*	72h	Platform-specific	Processor 07h	Sensor Specific 6Fh	01 - Thermal trip	Fatal	As and De	–	Trig Offset	M	X
					07 - Presence	OK					
Processor 4 Status *(P4 Status)*	73h	Platform-specific	Processor 07h	Sensor Specific 6Fh	01 - Thermal trip	Fatal	As and De	–	Trig Offset	M	X
					07 - Presence	OK					
Processor 1 Thermal Margin (P1 Therm Margin)	74h	All	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Processor 2 Thermal Margin (P2 Therm Margin)	75h	All	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Processor 3 Thermal Margin (P3 Therm Margin)	76h	Platform-specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Processor 4 Thermal Margin (P4 Therm Margin)	77h	Platform-specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
Processor 1 Thermal Control % (*P1 Therm Ctrl %*)	78h	All	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	Trig Offset	A	–
Processor 2 Thermal Control % (*P2 Therm Ctrl %*)	79h	All	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	Trig Offset	A	–
Processor 3 Thermal Control % (*P3 Therm Ctrl %*)	7Ah	Platform-specific	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	Trig Offset	A	–
Processor 4 Thermal Control % (*P4 Therm Ctrl %*)	7Bh	Platform-specific	Temperature 01h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	Trig Offset	A	–
Processor 1 ERR2 Timeout (P1 ERR2)	7Ch	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	fatal	As and De	–	Trig Offset	A	–
Processor 2 ERR2 Timeout (P2 ERR2)	7Dh	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	fatal	As and De	–	Trig Offset	A	–
Processor 3 ERR2 Timeout (P3 ERR2)	7Eh	Platform-specific	Processor 07h	Digital Discrete 03h	01 – State Asserted	fatal	As and De	–	Trig Offset	A	–
Processor 4 ERR2 Timeout (P4 ERR2)	7Fh	Platform-specific	Processor 07h	Digital Discrete 03h	01 – State Asserted	fatal	As and De	–	Trig Offset	A	–
Catastrophic Error *(CATERR)*	80h	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	fatal	As and De	–	Trig Offset	M	–
Processor1 MSID Mismatch *(P1 MSID Mismatch)*	81h	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	fatal	As and De	–	Trig Offset	M	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
Processor Population Fault *(CPU Missing)*	82h	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	M	–
Processor 1 DTS Thermal Margin (P1 DTS Therm Mgn)	83h	All	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Processor 2 DTS Thermal Margin (P2 DTS Therm Mgn)	84h	All	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Processor 3 DTS Thermal Margin (P3 DTS Therm Mgn)	85h	All	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Processor 4 DTS Thermal Margin (P4 DTS Therm Mgn)	86h	All	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Processor2 MSID Mismatch *(P2 MSID Mismatch)*	87h	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	fatal	As and De	–	Trig Offset	M	–
Processor 1 VRD Temperature (*P1 VRD Hot*)	90h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	M	–
Processor 2 VRD Temperature (*P2 VRD Hot*)	91h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	M	–
Processor 3 VRD Temperature (P3 VRD Hot)	92h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Fatal	As and De	–	Trig Offset	M	–
Processor 4 VRD Temperature (P4 VRD Hot)	93h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Fatal	As and De	–	Trig Offset	M	–
Processor 1 Memory VRD Hot 0-1 (P1 Mem01 VRD Hot)	94h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
Processor 1 Memory VRD Hot 2-3 (P1 Mem23 VRD Hot)	95h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 2 Memory VRD Hot 0-1 (P2 Mem01 VRD Hot)	96h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 2 Memory VRD Hot 2-3 (P2 Mem23 VRD Hot)	97h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 3 Memory VRD Hot 0-1 (P3 Mem01 VRD Hot)	98h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 3 Memory VRD Hot 2-3 (P4 Mem23 VRD Hot)	99h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 4 Memory VRD Hot 0-1 (P4 Mem01 VRD Hot)	9Ah	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Processor 4 Memory VRD Hot 2-3 (P4 Mem23 VRD Hot)	9Bh	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	–
Power Supply 1 Fan Tachometer 1 *(PS1 Fan Tach 1)*	A0h	Chassis-specific	Fan 04h	Generic – digital discrete	01 – State Asserted	Non-fatal	As and De	-	Trig Offset	M	-
Power Supply 1 Fan Tachometer 2 *(PS1 Fan Tach 2)*	A1h	Chassis-specific	Fan 04h	Generic – digital discrete	01 – State Asserted	Non-fatal	As and De	-	Trig Offset	M	-
Power Supply 2 Fan Tachometer 1 *(PS2 Fan Tach 1)*	A4h	Chassis-specific	Fan 04h	Generic – digital discrete	01 – State Asserted	Non-fatal	As and De	-	Trig Offset	M	-
Power Supply 2 Fan Tachometer 2 *(PS2 Fan Tach 2)*	A5h	Chassis-specific	Fan 04h	Generic – digital discrete	01 – State Asserted	Non-fatal	As and De	-	Trig Offset	M	-

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
Processor 1 DIMM Aggregate Thermal Margin 1 *(P1 DIMM Thrm Mrgn1)*	B0h	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Processor 1 DIMM Aggregate Thermal Margin 2 *(P1 DIMM Thrm Mrgn2)*	B1h	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Processor 2 DIMM Aggregate Thermal Margin 1 *(P2 DIMM Thrm Mrgn1)*	B2h	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Processor 2 DIMM Aggregate Thermal Margin 2 *(P2 DIMM Thrm Mrgn2)*	B3h	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Processor 3 DIMM Aggregate Thermal Margin 1 *(P3 DIMM Thrm Mrgn1)*	B4h	Platform Specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Processor 3 DIMM Aggregate Thermal Margin 2 *(P3 DIMM Thrm Mrgn2)*	B5h	Platform Specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Processor 4 DIMM Aggregate Thermal Margin 1 *(P4 DIMM Thrm Mrgn1)*	B6h	Platform Specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Processor 4 DIMM Aggregate Thermal Margin 2 *(P4 DIMM Thrm Mrgn2)*	B7h	Platform Specific	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
Fan Tachometer Sensors (Chassis specific sensor names)	BAh–BFh	Chassis and Platform Specific	Fan 04h	Threshold 01h	[l] [c,nc]	nc = Degraded c = Non-fatal[2]	As and De	Analog	R, T	M	-
Processor 1 DIMM Thermal Trip *(P1 Mem Thrm Trip)*	C0h	All	Memory 0Ch	Digital Discrete 03h	0A- Critical overtemperature	Fatal	As and De	–	Trig Offset	M	-
Processor 2 DIMM Thermal Trip *(P2 Mem Thrm Trip)*	C1h	All	Memory 0Ch	Digital Discrete 03h	0A- Critical overtemperature	Fatal	As and De	–	Trig Offset	M	-
Processor 3 DIMM Thermal Trip (P3 Mem Thrm Trip)	C2h	All	Memory 0Ch	Digital Discrete 03h	0A- Critical overtemperature	Fatal	As and De	–	Trig Offset	M	X
Processor 4 DIMM Thermal Trip (P4 Mem Thrm Trip)	C3h	All	Memory 0Ch	Digital Discrete 03h	0A- Critical overtemperature	Fatal	As and De	–	Trig Offset	M	X
Global Aggregate Temperature Margin 1 (Agg Therm Mrgn 1)	C8h	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Global Aggregate Temperature Margin 2 (Agg Therm Mrgn 2)	C9h	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Global Aggregate Temperature Margin 3 (Agg Therm Mrgn 3)	CAh	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Global Aggregate Temperature Margin 4 (Agg Therm Mrgn 4)	CBh	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Global Aggregate Temperature Margin 5 (Agg Therm Mrgn 5)	CCh	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Global Aggregate Temperature Margin 6 (Agg Therm Mrgn 6)	CDh	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
Global Aggregate Temperature Margin 7 (Agg Therm Mrgn 7)	CEh	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Global Aggregate Temperature Margin 8 (Agg Therm Mrgn 8)	CFh	Platform Specific	Temperature 01h	Threshold 01h	-	-	-	Analog	R, T	A	–
Baseboard +12V *(BB +12.0V)*	D0h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +5V *(BB +5.0V)*	D1h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +3.3V *(BB +3.3V)*	D2h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +5V Stand-by *(BB +5.0V STBY)*	D3h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Baseboard +3.3V Auxiliary *(BB +3.3V AUX)*	D4h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Baseboard +1.05V Processor1 Vccp *(BB +1.05Vccp P1)*	D6h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.05V Processor2 Vccp *(BB +1.05Vccp P2)*	D7h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.5V P1 Memory AB VDDQ *(BB +1.5 P1MEM AB)*	D8h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.5V P1 Memory CD VDDQ *(BB +1.5 P1MEM CD)*	D9h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
Baseboard +1.5V P2 Memory AB VDDQ *(BB +1.5 P2MEM AB)*	DAh	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.5V P2 Memory CD VDDQ *(BB +1.5 P2MEM CD)*	DBh	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.8V Aux (BB +1.8V AUX)	DCh	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.1V Stand-by (BB +1.1V STBY)	DDh	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard CMOS Battery *(BB +3.3V Vbat)*	DEh	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.35V P1 Low Voltage Memory AB VDDQ *(BB +1.35 P1LV AB)*	E4h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.35V P1 Low Voltage Memory CD VDDQ *(BB +1.35 P1LV CD)*	E5h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.35V P2 Low Voltage Memory AB VDDQ *(BB +1.35 P2LV AB)*	E6h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +1.35V P2 Low Voltage Memory CD VDDQ *(BB +1.35 P2LV CD)*	E7h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–

Full Sensor Name (Sensor name in SDR)	Sensor #	Platform Applicability	Sensor Type	Event/Reading Type	Event Offset Triggers	Contrib. To System Status	Assert/ De-assert	Readable Value / Offsets	Event Data	Rearm	Stand-by
Baseboard +3.3V Riser 1 Power Good (BB +3.3 RSR1 PGD)	EAh	Platform Specific	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard +3.3V Riser 2 Power Good (BB +3.3 RSR2 PGD)	EBh	Platform Specific	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Hard Disk Drive 1 -15 Status (HDD 1 - 15 Status)	F0h - FEh	Chassis -specific	Drive Slot 0Dh	Sensor Specific 6Fh	00 - Drive Presence	OK	As and De	–	Trig Offset	A	X
					01- Drive Fault	Degraded					
					07 - Rebuild/Remap in progress	Degraded					

Notes:

1. Redundancy sensors will be only present on systems with appropriate hardware to support redundancy (for instance, fan or power supply).
2. This is only applicable when the system doesn't support redundant fans. When fan redundancy is supported, then the contribution to system state is driven by the fan redundancy sensor.

Appendix C: Platform Specific BMC Appendix

Intel® Server Board S2600IP

Introduction

This is an addendum document to BMC core EPS. This document describes platform and chassis specific information.

Product ID

Bytes 11:12 (product ID) of Get Device ID command response: 55h 00h

IPMI Channel ID Assignments

The following table provides information on the BMC channel assignments:

Table 72. Intel® Server Board S2600IP - BMC Channel Assignments

Channel ID	Interface	Supports Sessions
0	Primary IPMB	Yes
1	LAN 1	Yes
2	LAN 2 (platform specific)	Yes
3	LAN3 [1] (Provided by the Intel® Dedicated Server Management NIC)	Yes
4	Reserved	Yes
5	USB	No
6	Secondary IPMB	No
7	SMM	No
8– 0Dh	Reserved	–
0Eh	Self [2]	–
0Fh	SMS / Receive Message Queue	No

Notes:

1. Optional HW supported by the server system.
2. Refers to the actual channel used to send the request.

ACPI S3 Sleep State Support

Not supported.

Processor Support for Intel® Server Board S2600IP

- Intel® Xeon® processor E5-2600 product family up to 135 Watt
- Intel® Xeon® processor E5-2600 v2 product family up to 135 Watt

Supported Chassis

- Intel® Server Chassis P4208 (UPL with redundant fan 4U)
- Intel® Server Chassis P4216 (UPL with redundant fan 4U)

- Intel® Server Chassis P4224 (UPL with redundant fan 4U)
- Intel® Server Chassis P4308 (UPL with redundant fan 4U)
- Intel® Server Chassis P4XXX (UPL with redundant fan 4U)
- Intel® Server Chassis R2208 (BHP with redundant fan 2U)
- Intel® Server Chassis R2216 (BHP with redundant fan 2U)
- Intel® Server Chassis R2224 (BHP with redundant fan 2U)
- Intel® Server Chassis R2308 (BHP with redundant fan 2U)
- Intel® Server Chassis R2312 (BHP with redundant fan 2U)

Chassis-specific sensors

Table 73. Intel® Server Board S2600IP - Chassis-specific Sensors

Intel® Server Chassis	Fan Tachometer Sensors	Fan Presence Sensors	Physical Security (Chassis intrusion) sensor	FP Interrupt (FP NMI Diag Int)
P4208/P4216/P4224/ P4308/P4XXX (UPL with redundant fan 4U)	System Fan 1(30h)	Fan 1 Present (40h)	Physical Scrty(04h)	FP NMI Diag Int (05h)
	System Fan 2(31h)	Fan 2 Present (41h)	NA	NA
	System Fan 3 (32h)	Fan 3 Present (42h)	NA	NA
	System Fan 4 (33h)	Fan 4 Present (43h)	NA	NA
	System Fan 5 (34h)	Fan 5 Present (44h)	NA	NA
R2208/R2216/R2224/P 2308/P2312 (BHP with redundant fan 2U)	System Fan 1 (30h)	Fan 1 Present (40h)	Physical Scrty(04h)	FP NMI Diag Int (05h)
	System Fan 2 (31h)	Fan 2 Present (41h)	NA	NA
	System Fan 3 (32h)	Fan 3 Present (42h)	NA	NA
	System Fan 4 (33h)	Fan 4 Present (43h)	NA	NA
	System Fan 5 (34h)	Fan 5 Present (44h)	NA	NA
	System Fan 6 (35h)	Fan 6 Present (45h)	NA	NA

Hot-plug fan support

Supported on:

- Intel® Server Chassis P4208 (UPL with redundant fan 4U)
- Intel® Server Chassis P4216 (UPL with redundant fan 4U)
- Intel® Server Chassis P4224 (UPL with redundant fan 4U)
- Intel® Server Chassis P4308 (UPL with redundant fan 4U)
- Intel® Server Chassis P4XXX (UPL with redundant fan 4U)
- Intel® Server Chassis R2208 (BHP with redundant fan 2U)
- Intel® Server Chassis R2216 (BHP with redundant fan 2U)
- Intel® Server Chassis R2224 (BHP with redundant fan 2U)
- Intel® Server Chassis R2308 (BHP with redundant fan 2U)
- Intel® Server Chassis R2312 (BHP with redundant fan 2U)

Fan redundancy support

Supported on:

- Intel® Server Chassis P4208 (UPL with redundant fan 4U)

- Intel® Server Chassis P4216 (UPL with redundant fan 4U)
- Intel® Server Chassis P4224 (UPL with redundant fan 4U)
- Intel® Server Chassis P4308 (UPL with redundant fan 4U)
- Intel® Server Chassis P4XXX (UPL with redundant fan 4U)
- Intel® Server Chassis R2208 (BHP with redundant fan 2U)
- Intel® Server Chassis R2216 (BHP with redundant fan 2U)
- Intel® Server Chassis R2224 (BHP with redundant fan 2U)
- Intel® Server Chassis R2308 (BHP with redundant fan 2U)
- Intel® Server Chassis R2312 (BHP with redundant fan 2U)

Fan domain definition

Table 74. Intel® Server Board S2600IP - Fan Domain Definition

Chassis	Fan Domain	Major Components Cooled (Temperature sensor number)	Fans (Sensor number)
P4208/P4216/P4224/P4308/P4XXX (UPL with redundant fan 4U)	0	▪ SSB Temp(22h) ▪ BB BMC Temp(23h) ▪ BB MEM VR Temp(25h) ▪ I/O Mod Temp(26h) ▪ HSBP 1 Temp(29h) ▪ HSBP 2 Temp(2Ah) ▪ SAS Mod Temp(2Dh) ▪ Exit Air Temp(2Eh) ▪ LAN NIC Temp(2Fh)	System Fan 1(30h)
	1	▪ SSB Temp(22h) ▪ BB BMC Temp(23h) ▪ BB MEM VR Temp(25h) ▪ I/O Mod Temp(26h) ▪ HSBP 1 Temp(29h) ▪ HSBP 2 Temp(2Ah) ▪ SAS Mod Temp(2Dh) ▪ Exit Air Temp(2Eh) ▪ LAN NIC Temp(2Fh)	System Fan 2(31h)
	2	▪ BB P2 VR Temp(24h) ▪ BB MEM VR Temp(25h) ▪ HSBP 1 Temp(29h) ▪ HSBP 2 Temp(2Ah) ▪ HSBP 3 Temp(2Bh) ▪ SAS Mod Temp(2Dh) ▪ Exit Air Temp(2Eh) ▪ HDD 20 Status(64h) ▪ HDD 21 Status(65h) ▪ DIMM Thrm Mrgn 2(B1h) ▪ DIMM Thrm Mrgn 3(B2h)	System Fan 3(32h)
	3	▪ BB P2 VR Temp(24h) ▪ HSBP 3 Temp(2Bh)	System Fan 4(33h)

Chassis	Fan Domain	Major Components Cooled (Temperature sensor number)	Fans (Sensor number)
		▪ Exit Air Temp(2Eh) ▪ P1 Therm Margin(74h) ▪ P2 Therm Margin(75h) ▪ DIMM Thrm Mrgn 1(B0h) ▪ DIMM Thrm Mrgn 4(B3h)	
	4	▪ BB P2 VR Temp(24h) ▪ HSBP 3 Temp(2Bh) ▪ Exit Air Temp(2Eh) ▪ PS1 Temperature(5Ch) ▪ PS2 Temperature(5Dh) ▪ HDD 20 Status(64h) ▪ HDD 21 Status(65h) ▪ DIMM Thrm Mrgn 1(B0h) ▪ DIMM Thrm Mrgn 4(B3h)	System Fan 5(34h)
R2208/R2216/R2224/P2308/P2312 (BHP with redundant fan 2U)	0	▪ SSB Temp(22h) ▪ BB BMC Temp(23h) ▪ BB MEM VR Temp(25h) ▪ I/O Mod Temp(26h) ▪ HSBP 1 Temp(29h) ▪ HSBP 2 Temp(2Ah) ▪ SAS Mod Temp(2Dh) ▪ Exit Air Temp(2Eh) ▪ LAN NIC Temp(2Fh)	System Fan 1(30h)
	1	▪ SSB Temp(22h) ▪ BB BMC Temp(23h) ▪ BB MEM VR Temp(25h) ▪ I/O Mod Temp(26h) ▪ HSBP 1 Temp(29h) ▪ HSBP 2 Temp(2Ah) ▪ SAS Mod Temp(2Dh) ▪ Exit Air Temp(2Eh) ▪ LAN NIC Temp(2Fh)	System Fan 2(31h)
	2	▪ SSB Temp(22h) ▪ BB P2 VR Temp(24h) ▪ HSBP 1 Temp(29h) ▪ HSBP 2 Temp(2Ah) ▪ P1 Therm Margin(74h) ▪ P2 Therm Margin(75h) ▪ P2 DTS Therm Mgn(84h) ▪ DIMM Thrm Mrgn 2(B1h) ▪ DIMM Thrm Mrgn 3(B2h)	System Fan 3(32h)
	3	▪ BB P2 VR Temp(24h) ▪ HSBP 1 Temp(29h) ▪ HSBP 2 Temp(2Ah) ▪ HSBP 3 Temp(2Bh) ▪ Exit Air Temp(2Eh)	System Fan 4(33h)

Chassis	Fan Domain	Major Components Cooled (Temperature sensor number)	Fans (Sensor number)
		▪ P1 Therm Margin(74h) ▪ P2 Therm Margin(75h) ▪ DIMM Thrm Mrgn 1(B0h) ▪ DIMM Thrm Mrgn 2(B1h) ▪ DIMM Thrm Mrgn 3(B2h) ▪ DIMM Thrm Mrgn 4(B3h)	
	4	▪ SSB Temp(22h) ▪ BB P2 VR Temp(24h) ▪ HSBP 1 Temp(29h) ▪ HSBP 2 Temp(2Ah) ▪ P1 Therm Margin(74h) ▪ P2 Therm Margin(75h) ▪ P2 DTS Therm Mgn(84h) ▪ DIMM Thrm Mrgn 2(B1h) ▪ DIMM Thrm Mrgn 3(B2h)	System Fan 5(34h)
	5	▪ BB P2 VR Temp(24h) ▪ HSBP 1 Temp(29h) ▪ HSBP 2 Temp(2Ah) ▪ HSBP 3 Temp(2Bh) ▪ Exit Air Temp(2Eh) ▪ P1 Therm Margin(74h) ▪ P2 Therm Margin(75h) ▪ DIMM Thrm Mrgn 1(B0h) ▪ DIMM Thrm Mrgn 2(B1h) ▪ DIMM Thrm Mrgn 3(B2h) ▪ DIMM Thrm Mrgn 4(B3h)	System Fan 6(35h)

HSC Availability

- Intel® Server Chassis P4208 (UPL)
  - 8-bay 2.5” HDD – FXX8X25HSBP
- Intel® Server Chassis P4216 (UPL)
  - 8-bay 2.5” HDD – FXX8X25HSBP
- Intel® Server Chassis P4224 (UPL)
  - 8-bay 2.5” HDD – FXX8X25HSBP
- Intel® Server Chassis P4308 (UPL)
  - 8-bay 3.5” HDD – FUP8X35HSBP
- Intel® Server Chassis R2208 (BHP)
  - 8-bay 2.5” HDD – FXX8X25HSBP
- Intel® Server Chassis R2216 (BHP)
  - 8-bay 2.5” HDD – FXX8X25HSBP
- Intel® Server Chassis R2224 (BHP)
  - 8-bay 2.5” HDD – FXX8X25HSBP
- Intel® Server Chassis R2308 (BHP)

  - 8-bay 3.5” HDD – F2U8X35HSBP
- Intel® Server Chassis R2312 (BHP)
  - 12-bay 3.5” HDD – F2U12X35HSBP

Power unit support

- Intel® Server Chassis P4208/P4216/P4224/P4308 (UPL)

Table 75. Intel® Server Chassis P4208/P4216/P4224/P4308 (UPL) Power support

PS Module Number	PMBus	Product Name (in product area of the FRU)	PSU Redundant	Cold Redundant	Fans in each PS
750W HS Power Supply	Supported	DPS-750XB A	Supported	Supported	1 PS fan
1200W HS Power Supply	Supported	DPS-1200TB A	Supported	Supported	2 PS fan

- Intel® Server Chassis R2208/R2216/R2224/R2308/R2312 (BHP)

Table 76. Intel® Server Chassis R2208/R2216/R2224/R2308/R2312 (BHP) Power support

PS Module Number	PMBus	Product Name(in product area of the FRU)	PSU Redundant	Cold Redundant	Fans in each PS
750W HS Power Supply	Supported	FS750HS1-00	Supported	Supported	1 PS fan

Redundant Fans only for Intel® Server Chassis

- Intel® Server Chassis P4208 (UPL with redundant fan 4U)
- Intel® Server Chassis P4216 (UPL with redundant fan 4U)
- Intel® Server Chassis P4224 (UPL with redundant fan 4U)
- Intel® Server Chassis P4308 (UPL with redundant fan 4U)
- Intel® Server Chassis P4XXX (UPL with redundant fan 4U)
- Intel® Server Chassis R2208 (BHP with redundant fan 2U)
- Intel® Server Chassis R2216 (BHP with redundant fan 2U)
- Intel® Server Chassis R2224 (BHP with redundant fan 2U)
- Intel® Server Chassis R2308 (BHP with redundant fan 2U)
- Intel® Server Chassis R2312 (BHP with redundant fan 2U)

Fan Fault LED support

Fan fault LEDs are available on the baseboard and on the hot-swap redundant fans available on the following chassis:

- Intel® Server Chassis P4208 (UPL with redundant fan 4U)
- Intel® Server Chassis P4216 (UPL with redundant fan 4U)
- Intel® Server Chassis P4224 (UPL with redundant fan 4U)

- Intel® Server Chassis P4308 (UPL with redundant fan 4U)
- Intel® Server Chassis P4XXX (UPL with redundant fan 4U)
- Intel® Server Chassis R2208 (BHP with redundant fan 2U)
- Intel® Server Chassis R2216 (BHP with redundant fan 2U)
- Intel® Server Chassis R2224 (BHP with redundant fan 2U)
- Intel® Server Chassis R2308 (BHP with redundant fan 2U)
- Intel® Server Chassis R2312 (BHP with redundant fan 2U)

Memory Throttling support

- Baseboard supports this feature.

Intel® Workstation Board W2600CR

Introduction

This is an addendum document to BMC core EPS. This document describes platform and chassis specific information.

Product ID

Bytes 11:12 (product ID) of Get Device ID command response: 56h 00h

IPMI Channel ID Assignments

The following table provides information on the BMC channel assignments:

Table 77. Intel® Workstation Board W2600CR - BMC Channel Assignments

Channel ID	Interface	Supports Sessions
0	Primary IPMB	Yes
1	LAN 1	Yes
2	LAN 2 (platform specific)	Yes
3	LAN3 [1] (Provided by the Intel® Dedicated Server Management NIC)	Yes
4	Reserved	Yes
5	USB	No
6	Secondary IPMB	No
7	SMM	No
8– 0Dh	Reserved	–
0Eh	Self [2]	–
0Fh	SMS / Receive Message Queue	No

Notes:

1. Optional HW supported by the server system.
2. Refers to the actual channel used to send the request.

ACPI S3 Sleep State Support

Supported

Processor Support for Intel® Server Board W2600CR

- Intel® Xeon® processor E5-2600 product family up to 150 Watt
- Intel® Xeon® processor E5-2600 v2 product family up to 150 Watt

Supported Chassis

- Intel® Server Chassis P4304 (UPL with fixed fan 4U)

Chassis-specific sensors

Table 78. Intel® Workstation Board W2600CR - Chassis-specific sensors

Intel® Server Chassis	Fan Tachometer Sensors	Fan Presene Sensors	Physical Security (Chassis intrusion) sensor	FP Interrupt (FP NMI Diag Int)
P4304 (UPL with fixed fan 4U)	System Fan 1(30h)	NA	Physical Scrty(04h)	FP NMI Diag Int(05h)
	System Fan 2(31h)	NA	NA	NA
	Processor 1 Fan (36h)	NA	NA	NA
	Processor 2 Fan (37h)detected	NA	NA	NA

Hot-plug fan support

Not supported.

Fan redundancy support

Not supported.

Board specific feature

Board has not supported serial port A, and SOL will only use serial port B.

Fan domain definition

Table 79. Intel® Workstation Board W2600CR - Fan domain definition

Chassis	Fan Domain	Major Components Cooled (Temperature sensor number)	Fans (Sensor number)
P4304 (UPL with fixed fan 4U)	0	▪ SSB Temp(22h) ▪ BB BMC Temp(23h) ▪ BB MEM VR Temp(25h) ▪ I/O Mod Temp(26h) ▪ SAS Mod Temp(2Dh) ▪ Exit Air Temp(2Eh) ▪ LAN NIC Temp(2Fh) ▪ DIMM Thrm Mrgn 2(B1h) ▪ DIMM Thrm Mrgn 3(B2h)	System Fan 1(30h)
	1	▪ BB P2 VR Temp(24h) ▪ BB MEM VR Temp(25h)	System Fan 2(31h)

Chassis	Fan Domain	Major Components Cooled (Temperature sensor number)	Fans (Sensor number)
		▪ Exit Air Temp(2Eh) ▪ HDD 20 Status(64h) ▪ HDD 21 Status(65h) ▪ DIMM Thrm Mrgn 1(B0h) ▪ DIMM Thrm Mrgn 2(B1h) ▪ DIMM Thrm Mrgn 3(B2h) ▪ DIMM Thrm Mrgn 4(B3h)	
	6	▪ Exit Air Temp(2Eh) ▪ P1 Therm Margin(74h)	Processor 1 Fan(36h)
	7	▪ BB P2 VR Temp(24h) ▪ Exit Air Temp(2Eh) ▪ P2 Therm Margin(75h)	Processor 2 Fan(37h)

HSC Availability

Not supported.

Power unit support

- Intel® Server Chassis P4304 (UPL)

Table 80. Intel® Server Chassis P4304 (UPL) Power support

PS Module Number	PMBus	Product Name (in product area of the FRU)	PSU Redundant	Cold Redundant	Fans in each PS
750W HS Power Supply	Supported	DPS-750XB A	Supported	Supported	1 PS fan
1200W HS Power Supply	Supported	DPS-1200TB A	Supported	Supported	2PS fan

Redundant Fans only for Intel® Server Chassis

Not supported.

Fan Fault LED support

Not supported.

Memory Throttling support

- Baseboard supports this feature.

Appendix D: POST Code Diagnostic LED Decoder

During the system boot process, the BIOS executes a number of platform configuration processes, each of which is assigned a specific hex POST code number. As each configuration routine is started, the BIOS displays the POST code to the POST Code Diagnostic LEDs on the back edge of the server board. To assist in troubleshooting a system hang during the POST process, the Diagnostic LEDs can be used to identify the last POST process that was executed.

Each POST code is represented by a sequence of eight amber diagnostic LEDs. The POST codes are divided into two nibbles, an upper nibble and a lower nibble. The upper nibble bits are represented by diagnostic LEDs #4, #5, #6, and #7. The lower nibble bits are represented by diagnostics LEDs #0, #1, #2, and #3. If the bit is set in the upper and lower nibbles, then the corresponding LED is lit. If the bit is clear, then the corresponding LED is off.

The diagnostic LED #7 is labeled as “MSB”, and the diagnostic LED #0 is labeled as “LSB”.

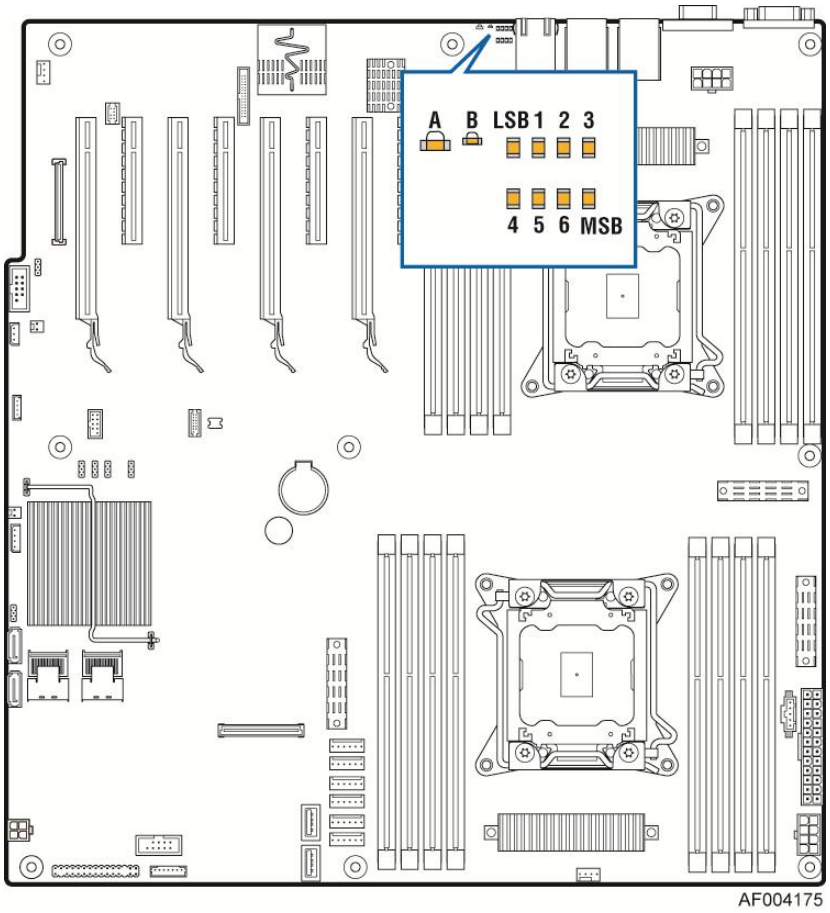


Figure 36. POST Code Diagnostic LED Decoder

Note: Diagnostic LEDs are best read and decoded when viewing the LEDs from the back of the system

Table 81. POST Progress Code LED Example

LEDs	Upper Nibble AMBER LEDs				Lower Nibble GREEN LEDs			
	MSB							LSB
	LED #7	LED #6	LED #5	LED #4	LED #3	LED #2	LED #1	LED #0
	8h	4h	2h	1h	8h	4h	2h	1h
Status	ON	OFF	ON	OFF	ON	ON	OFF	OFF
Results	1	0	1	0	1	1	0	0
	Ah				**Ch**			

Upper nibble bits = 1010b = Ah; Lower nibble bits = 1100b = Ch; the two are concatenated as ACh

The following table provides a list of all POST progress codes.

Table 82. POST Progress Codes

Checkpoint	Diagnostic LED Decoder 1 = LED On, 0 = LED Off								Description
	Upper Nibble				Lower Nibble				
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED #	#7	#6	#5	#4	#3	#2	#1	#0	
SEC Phase									
01h	0	0	0	0	0	0	0	1	First POST code after CPU reset
02h	0	0	0	0	0	0	1	0	Microcode load begin
03h	0	0	0	0	0	0	1	1	CRAM initialization begin
04h	0	0	0	0	0	1	0	0	Pei Cache When Disabled
05h	0	0	0	0	0	1	0	1	SEC Core At Power On Begin.
06h	0	0	0	0	0	1	1	0	Early CPU initialization during Sec Phase.
07h	0	0	0	0	0	1	1	1	Early SB initialization during Sec Phase.
08h	0	0	0	0	1	0	0	0	Early NB initialization during Sec Phase.
09h	0	0	0	0	1	0	0	1	End Of Sec Phase.
0Eh	0	0	0	0	1	1	1	0	Microcode Not Found.
0Fh	0	0	0	0	1	1	1	1	Microcode Not Loaded.
PEI Phase									
10h	0	0	0	1	0	0	0	0	PEI Core
11h	0	0	0	1	0	0	0	1	CPU PEIM
15h	0	0	0	1	0	1	0	1	NB PEIM
19h	0	0	0	1	1	0	0	1	SB PEIM
MRC Process Codes – MRC Progress Code Sequence is executed - See Table 63									
PEI Phase continued…									
31h	0	0	1	1	0	0	0	1	Memory Installed
32h	0	0	1	1	0	0	1	0	CPU PEIM (Cpu Init)
33h	0	0	1	1	0	0	1	1	CPU PEIM (Cache Init)
34h	0	0	1	1	0	1	0	0	CPU PEIM (BSP Select)
35h	0	0	1	1	0	1	0	1	CPU PEIM (AP Init)
36h	0	0	1	1	0	1	1	0	CPU PEIM (CPU SMM Init)
4Fh	0	1	0	0	1	1	1	1	Dxe IPL started
DXE Phase									
60h	0	1	1	0	0	0	0	0	DXE Core started
61h	0	1	1	0	0	0	0	1	DXE NVRAM Init

Checkpoint	Diagnostic LED Decoder 1 = LED On, 0 = LED Off								
	Upper Nibble				Lower Nibble				
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED #	#7	#6	#5	#4	#3	#2	#1	#0	Description
62h	0	1	1	0	0	0	1	0	SB RUN Init
63h	0	1	1	0	0	0	1	1	Dxe CPU Init
68h	0	1	1	0	1	0	0	0	DXE PCI Host Bridge Init
69h	0	1	1	0	1	0	0	1	DXE NB Init
6Ah	0	1	1	0	1	0	1	0	DXE NB SMM Init
70h	0	1	1	1	0	0	0	0	DXE SB Init
71h	0	1	1	1	0	0	0	1	DXE SB SMM Init
72h	0	1	1	1	0	0	1	0	DXE SB devices Init
78h	0	1	1	1	1	0	0	0	DXE ACPI Init
79h	0	1	1	1	1	0	0	1	DXE CSM Init
90h	1	0	0	1	0	0	0	0	DXE BDS Started
91h	1	0	0	1	0	0	0	1	DXE BDS connect drivers
92h	1	0	0	1	0	0	1	0	DXE PCI Bus begin
93h	1	0	0	1	0	0	1	1	DXE PCI Bus HPC Init
94h	1	0	0	1	0	1	0	0	DXE PCI Bus enumeration
95h	1	0	0	1	0	1	0	1	DXE PCI Bus resource requested
96h	1	0	0	1	0	1	1	0	DXE PCI Bus assign resource
97h	1	0	0	1	0	1	1	1	DXE CON_OUT connect
98h	1	0	0	1	1	0	0	0	DXE CON_IN connect
99h	1	0	0	1	1	0	0	1	DXE SIO Init
9Ah	1	0	0	1	1	0	1	0	DXE USB start
9Bh	1	0	0	1	1	0	1	1	DXE USB reset
9Ch	1	0	0	1	1	1	0	0	DXE USB detect
9Dh	1	0	0	1	1	1	0	1	DXE USB enable
A1h	1	0	1	0	0	0	0	1	DXE IDE begin
A2h	1	0	1	0	0	0	1	0	DXE IDE reset
A3h	1	0	1	0	0	0	1	1	DXE IDE detect
A4h	1	0	1	0	0	1	0	0	DXE IDE enable
A5h	1	0	1	0	0	1	0	1	DXE SCSI begin
A6h	1	0	1	0	0	1	1	0	DXE SCSI reset
A7h	1	0	1	0	0	1	1	1	DXE SCSI detect
A8h	1	0	1	0	1	0	0	0	DXE SCSI enable
A9h	1	0	1	0	1	0	0	1	DXE verifying SETUP password
ABh	1	0	1	0	1	0	1	1	DXE SETUP start
ACh	1	0	1	0	1	1	0	0	DXE SETUP input wait
ADh	1	0	1	0	1	1	0	1	DXE Ready to Boot
AEh	1	0	1	0	1	1	1	0	DXE Legacy Boot
AFh	1	0	1	0	1	1	1	1	DXE Exit Boot Services
B0h	1	0	1	1	0	0	0	0	RT Set Virtual Address Map Begin
B1h	1	0	1	1	0	0	0	1	RT Set Virtual Address Map End

Checkpoint	Diagnostic LED Decoder 1 = LED On, 0 = LED Off								
	Upper Nibble				Lower Nibble				
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED #	#7	#6	#5	#4	#3	#2	#1	#0	Description
B2h	1	0	1	1	0	0	1	0	DXE Legacy Option ROM init
B3h	1	0	1	1	0	0	1	1	DXE Reset system
B4h	1	0	1	1	0	1	0	0	DXE USB Hot plug
B5h	1	0	1	1	0	1	0	1	DXE PCI BUS Hot plug
B6h	1	0	1	1	0	1	1	0	DXE NVRAM cleanup
B7h	1	0	1	1	0	1	1	1	DXE Configuration Reset
00h	0	0	0	0	0	0	0	0	INT19
S3 Resume									
E0h	1	1	0	1	0	0	0	0	S3 Resume PEIM (S3 started)
E1h	1	1	0	1	0	0	0	1	S3 Resume PEIM (S3 boot script)
E2h	1	1	0	1	0	0	1	0	S3 Resume PEIM (S3 Video Repost)
E3h	1	1	0	1	0	0	1	1	S3 Resume PEIM (S3 OS wake)
BIOS Recovery									
F0h	1	1	1	1	0	0	0	0	PEIM which detected forced Recovery condition
F1h	1	1	1	1	0	0	0	1	PEIM which detected User Recovery condition
F2h	1	1	1	1	0	0	1	0	Recovery PEIM (Recovery started)
F3h	1	1	1	1	0	0	1	1	Recovery PEIM (Capsule found)
F4h	1	1	1	1	0	1	0	0	Recovery PEIM (Capsule loaded)

POST Memory Initialization MRC Diagnostic Codes

There are two types of POST Diagnostic Codes displayed by the MRC during memory initialization; Progress Codes and Fatal Error Codes.

The MRC Progress Codes are displays to the Diagnostic LEDs that show the execution point in the MRC operational path at each step.

Table 83. MRC Progress Codes

Checkpoint	Diagnostic LED Decoder 1 = LED On, 0 = LED Off								Description
	Upper Nibble				Lower Nibble				
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
MRC Progress Codes									
B0h	1	0	1	1	0	0	0	0	Detect DIMM population
B1h	1	0	1	1	0	0	0	1	Set DDR3 frequency
B2h	1	0	1	1	0	0	1	0	Gather remaining SPD data
B3h	1	0	1	1	0	0	1	1	Program registers on the memory controller level
B4h	1	0	1	1	0	1	0	0	Evaluate RAS modes and save rank information

Checkpoint	Diagnostic LED Decoder								Description
	1 = LED On, 0 = LED Off								
	Upper Nibble				Lower Nibble				
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
B5h	1	0	1	1	0	1	0	1	Program registers on the channel level
B6h	1	0	1	1	0	1	1	0	Perform the JEDEC defined initialization sequence
B7h	1	0	1	1	0	1	1	1	Train DDR3 ranks
B8h	1	0	1	1	1	0	0	0	Initialize CLTT/OLTT
B9h	1	0	1	1	1	0	0	1	Hardware memory test and init
BAh	1	0	1	1	1	0	1	0	Execute software memory init
BBh	1	0	1	1	1	0	1	1	Program memory map and interleaving
BCh	1	0	1	1	1	1	0	0	Program RAS configuration
BFh	1	0	1	1	1	1	1	1	MRC is done

Memory Initialization at the beginning of POST includes multiple functions, including: discovery, channel training, validation that the DIMM population is acceptable and functional, initialization of the IMC and other hardware settings, and initialization of applicable RAS configurations.

When a major memory initialization error occurs and prevents the system from booting with data integrity, a beep code is generated, the MRC will display a fatal error code on the diagnostic LEDs, and a system halt command is executed. Fatal MRC error halts do NOT change the state of the System Status LED, and they do NOT get logged as SEL events. The following table lists all MRC fatal errors that are displayed to the Diagnostic LEDs.

Table 84. MRC Fatal Error Codes

Checkpoint	Diagnostic LED Decoder								Description
	1 = LED On, 0 = LED Off								
	Upper Nibble				Lower Nibble				
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
MRC Fatal Error Codes									
E8h	1	1	1	0	1	0	0	0	No usable memory error 01h = No memory was detected by SPD read, or invalid config that causes no operable memory. 02h = Memory DIMMs on all channels of all sockets are disabled due to hardware memtest error. 3h = No memory installed. All channels are disabled.
E9h	1	1	1	0	1	0	0	1	Memory is locked by Intel Trusted Execuiton Technology and is inaccessible
EAh	1	1	1	0	1	0	1	0	DDR3 channel training error 01h = Error on read DQ/DQS (Data/Data Strobe) init 02h = Error on Receive Enable 3h = Error on Write Leveling 04h = Error on write DQ/DQS (Data/Data Strobe
EBh	1	1	1	0	1	0	1	1	Memory test failure 01h = Software memtest failure.

Checkpoint	Diagnostic LED Decoder								Description
	1 = LED On, 0 = LED Off								
	Upper Nibble				Lower Nibble				
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
									02h = Hardware memtest failed. 03h = Hardware Memtest failure in Lockstep Channel mode requiring a channel to be disabled. *This is a fatal error which requires a reset and calling MRC with a different RAS mode to retry.*
EDh	1	1	1	0	1	1	0	1	DIMM configuration population error 01h = Different DIMM types (UDIMM, RDIMM, LRDIMM) are detected installed in the system. 02h = Violation of DIMM population rules. 03h = The 3rd DIMM slot cannot be populated when QR DIMMs are installed. 04h = UDIMMs are not supported in the 3rd DIMM slot. 05h = Unsupported DIMM Voltage.
EFh	1	1	1	0	1	1	1	1	Indicates a CLTT table structure error

Appendix E: POST Error Messages and Handling

Most error conditions encountered during POST are reported using **POST Error Codes**. These codes represent specific failures, warnings, or are informational. POST Error Codes may be displayed in the Error Manager display screen, and are always logged to the System Event Log (SEL). Logged events are available to System Management applications, including Remote and Out of Band (OOB) management.

There are exception cases in early initialization where system resources are not adequately initialized for handling POST Error Code reporting. These cases are primarily Fatal Error conditions resulting from initialization of processors and memory, and they are handed by a Diagnostic LED display with a system halt.

The following table lists the supported POST Error Codes. Each error code is assigned an error type which determines the action the BIOS will take when the error is encountered. Error types include Minor, Major, and Fatal. The BIOS action for each is defined as follows:

- **Minor:** The error message is displayed on the screen or on the Error Manager screen, and an error is logged to the SEL. The system continues booting in a degraded state. The user may want to replace the erroneous unit. The POST Error Pause option setting in the BIOS setup does not have any effect on this error.
- **Major:** The error message is displayed on the Error Manager screen, and an error is logged to the SEL. The POST Error **Pause** option setting in the BIOS setup determines whether the system pauses to the Error Manager for this type of error so the user can take immediate corrective action or the system continues booting.

  Note that for 0048 “Password check failed”, the system halts, and then after the next reset/reboot will displays the error code on the Error Manager screen.

- **Fatal:** The system halts during post at a blank screen with the text **“Unrecoverable fatal error found. System will not boot until the error is resolved”** and **“Press <F2> to enter setup”** The POST Error Pause option setting in the BIOS setup does not have any effect with this class of error.

  When the operator presses the **F2** key on the keyboard, the error message is displayed on the Error Manager screen, and an error is logged to the SEL with the error code. The system cannot boot unless the error is resolved. The user needs to replace the faulty part and restart the system.

Note: The POST error codes in the following table are common to all current generation Intel server platforms. Features present on a given server board/system will determine which of the listed error codes are supported.

Table 85. POST Error Codes and Messages

Error Code	Error Message	Response
0012	System RTC date/time not set	Major
0048	Password check failed	Major
0140	PCI component encountered a PERR error	Major

Error Code	Error Message	Response
0141	PCI resource conflict	Major
0146	PCI out of resources error	Major
0191	Processor core/thread count mismatch detected	Fatal
0192	Processor cache size mismatch detected	Fatal
0194	Processor family mismatch detected	Fatal
0195	Processor Intel(R) QPI link frequencies unable to synchronize	Fatal
0196	Processor model mismatch detected	Fatal
0197	Processor frequencies unable to synchronize	Fatal
5220	BIOS Settings reset to default settings	Major
5221	Passwords cleared by jumper	Major
5224	Password clear jumper is Set	Major
8130	Processor 01 disabled	Major
8131	Processor 02 disabled	Major
8132	Processor 03 disabled	Major
8133	Processor 04 disabled	Major
8160	Processor 01 unable to apply microcode update	Major
8161	Processor 02 unable to apply microcode update	Major
8162	Processor 03 unable to apply microcode update	Major
8163	Processor 04 unable to apply microcode update	Major
8170	Processor 01 failed Self Test (BIST)	Major
8171	Processor 02 failed Self Test (BIST)	Major
8172	Processor 03 failed Self Test (BIST)	Major
8173	Processor 04 failed Self Test (BIST)	Major
8180	Processor 01 microcode update not found	Minor
8181	Processor 02 microcode update not found	Minor
8182	Processor 03 microcode update not found	Minor
8183	Processor 04 microcode update not found	Minor
8190	Watchdog timer failed on last boot	Major
8198	OS boot watchdog timer failure	Major
8300	Baseboard management controller failed self-test	Major
8305	Hot Swap Controller failure	Major
83A0	Management Engine (ME) failed Selftest	Major
83A1	Management Engine (ME) Failed to respond.	Major
84F2	Baseboard management controller failed to respond	Major
84F3	Baseboard management controller in update mode	Major
84F4	Sensor data record empty	Major
84FF	System event log full	Minor
8500	Memory component could not be configured in the selected RAS mode	Major
8501	DIMM Population Error	Major
8520	DIMM_A1 failed test/initialization	Major
8521	DIMM_A2 failed test/initialization	Major
8522	DIMM_A3 failed test/initialization	Major
8523	DIMM_B1 failed test/initialization	Major
8524	DIMM_B2 failed test/initialization	Major
8525	DIMM_B3 failed test/initialization	Major
8526	DIMM_C1 failed test/initialization	Major

Error Code	Error Message	Response
8527	DIMM_C2 failed test/initialization	Major
8528	DIMM_C3 failed test/initialization	Major
8529	DIMM_D1 failed test/initialization	Major
852A	DIMM_D2 failed test/initialization	Major
852B	DIMM_D3 failed test/initialization	Major
852C	DIMM_E1 failed test/initialization	Major
852D	DIMM_E2 failed test/initialization	Major
852E	DIMM_E3 failed test/initialization	Major
852F	DIMM_F1 failed test/initialization	Major
8530	DIMM_F2 failed test/initialization	Major
8531	DIMM_F3 failed test/initialization	Major
8532	DIMM_G1 failed test/initialization	Major
8533	DIMM_G2 failed test/initialization	Major
8534	DIMM_G3 failed test/initialization	Major
8535	DIMM_H1 failed test/initialization	Major
8536	DIMM_H2 failed test/initialization	Major
8537	DIMM_H3 failed test/initialization	Major
8538	DIMM_I1 failed test/initialization	Major
8539	DIMM_I2 failed test/initialization	Major
853A	DIMM_I3 failed test/initialization	Major
853B	DIMM_J1 failed test/initialization	Major
853C	DIMM_J2 failed test/initialization	Major
853D	DIMM_J3 failed test/initialization	Major
853E	DIMM_K1 failed test/initialization	Major
853F (Go to 85C0)	DIMM_K2 failed test/initialization	Major
8540	DIMM_A1 disabled	Major
8541	DIMM_A2 disabled	Major
8542	DIMM_A3 disabled	Major
8543	DIMM_B1 disabled	Major
8544	DIMM_B2 disabled	Major
8545	DIMM_B3 disabled	Major
8546	DIMM_C1 disabled	Major
8547	DIMM_C2 disabled	Major
8548	DIMM_C3 disabled	Major
8549	DIMM_D1 disabled	Major
854A	DIMM_D2 disabled	Major
854B	DIMM_D3 disabled	Major
854C	DIMM_E1 disabled	Major
854D	DIMM_E2 disabled	Major
854E	DIMM_E3 disabled	Major
854F	DIMM_F1 disabled	Major
8550	DIMM_F2 disabled	Major
8551	DIMM_F3 disabled	Major
8552	DIMM_G1 disabled	Major
8553	DIMM_G2 disabled	Major

Error Code	Error Message	Response
8554	DIMM_G3 disabled	Major
8555	DIMM_H1 disabled	Major
8556	DIMM_H2 disabled	Major
8557	DIMM_H3 disabled	Major
8558	DIMM_I1 disabled	Major
8559	DIMM_I2 disabled	Major
855A	DIMM_I3 disabled	Major
855B	DIMM_J1 disabled	Major
855C	DIMM_J2 disabled	Major
855D	DIMM_J3 disabled	Major
855E	DIMM_K1 disabled	Major
855F (Go to 85D0)	DIMM_K2 disabled	Major
8560	DIMM_A1 encountered a Serial Presence Detection (SPD) failure	Major
8561	DIMM_A2 encountered a Serial Presence Detection (SPD) failure	Major
8562	DIMM_A3 encountered a Serial Presence Detection (SPD) failure	Major
8563	DIMM_B1 encountered a Serial Presence Detection (SPD) failure	Major
8564	DIMM_B2 encountered a Serial Presence Detection (SPD) failure	Major
8565	DIMM_B3 encountered a Serial Presence Detection (SPD) failure	Major
8566	DIMM_C1 encountered a Serial Presence Detection (SPD) failure	Major
8567	DIMM_C2 encountered a Serial Presence Detection (SPD) failure	Major
8568	DIMM_C3 encountered a Serial Presence Detection (SPD) failure	Major
8569	DIMM_D1 encountered a Serial Presence Detection (SPD) failure	Major
856A	DIMM_D2 encountered a Serial Presence Detection (SPD) failure	Major
856B	DIMM_D3 encountered a Serial Presence Detection (SPD) failure	Major
856C	DIMM_E1 encountered a Serial Presence Detection (SPD) failure	Major
856D	DIMM_E2 encountered a Serial Presence Detection (SPD) failure	Major
856E	DIMM_E3 encountered a Serial Presence Detection (SPD) failure	Major
856F	DIMM_F1 encountered a Serial Presence Detection (SPD) failure	Major
8570	DIMM_F2 encountered a Serial Presence Detection (SPD) failure	Major
8571	DIMM_F3 encountered a Serial Presence Detection (SPD) failure	Major
8572	DIMM_G1 encountered a Serial Presence Detection (SPD) failure	Major
8573	DIMM_G2 encountered a Serial Presence Detection (SPD) failure	Major
8574	DIMM_G3 encountered a Serial Presence Detection (SPD) failure	Major
8575	DIMM_H1 encountered a Serial Presence Detection (SPD) failure	Major
8576	DIMM_H2 encountered a Serial Presence Detection (SPD) failure	Major
8577	DIMM_H3 encountered a Serial Presence Detection (SPD) failure	Major
8578	DIMM_I1 encountered a Serial Presence Detection (SPD) failure	Major
8579	DIMM_I2 encountered a Serial Presence Detection (SPD) failure	Major
857A	DIMM_I3 encountered a Serial Presence Detection (SPD) failure	Major
857B	DIMM_J1 encountered a Serial Presence Detection (SPD) failure	Major
857C	DIMM_J2 encountered a Serial Presence Detection (SPD) failure	Major
857D	DIMM_J3 encountered a Serial Presence Detection (SPD) failure	Major
857E	DIMM_K1 encountered a Serial Presence Detection (SPD) failure	Major
857F (Go to 85E0)	DIMM_K2 encountered a Serial Presence Detection (SPD) failure	Major

Error Code	Error Message	Response
85C0	DIMM_K3 failed test/initialization	Major
85C1	DIMM_L1 failed test/initialization	Major
85C2	DIMM_L2 failed test/initialization	Major
85C3	DIMM_L3 failed test/initialization	Major
85C4	DIMM_M1 failed test/initialization	Major
85C5	DIMM_M2 failed test/initialization	Major
85C6	DIMM_M3 failed test/initialization	Major
85C7	DIMM_N1 failed test/initialization	Major
85C8	DIMM_N2 failed test/initialization	Major
85C9	DIMM_N3 failed test/initialization	Major
85CA	DIMM_O1 failed test/initialization	Major
85CB	DIMM_O2 failed test/initialization	Major
85CC	DIMM_O3 failed test/initialization	Major
85CD	DIMM_P1 failed test/initialization	Major
85CE	DIMM_P2 failed test/initialization	Major
85CF	DIMM_P3 failed test/initialization	Major
85D0	DIMM_K3 disabled	Major
85D1	DIMM_L1 disabled	Major
85D2	DIMM_L2 disabled	Major
85D3	DIMM_L3 disabled	Major
85D4	DIMM_M1 disabled	Major
85D5	DIMM_M2 disabled	Major
85D6	DIMM_M3 disabled	Major
85D7	DIMM_N1 disabled	Major
85D8	DIMM_N2 disabled	Major
85D9	DIMM_N3 disabled	Major
85DA	DIMM_O1 disabled	Major
85DB	DIMM_O2 disabled	Major
85DC	DIMM_O3 disabled	Major
85DD	DIMM_P1 disabled	Major
85DE	DIMM_P2 disabled	Major
85DF	DIMM_P3 disabled	Major
85E0	DIMM_K3 encountered a Serial Presence Detection (SPD) failure	Major
85E1	DIMM_L1 encountered a Serial Presence Detection (SPD) failure	Major
85E2	DIMM_L2 encountered a Serial Presence Detection (SPD) failure	Major
85E3	DIMM_L3 encountered a Serial Presence Detection (SPD) failure	Major
85E4	DIMM_M1 encountered a Serial Presence Detection (SPD) failure	Major
85E5	DIMM_M2 encountered a Serial Presence Detection (SPD) failure	Major
85E6	DIMM_M3 encountered a Serial Presence Detection (SPD) failure	Major
85E7	DIMM_N1 encountered a Serial Presence Detection (SPD) failure	Major
85E8	DIMM_N2 encountered a Serial Presence Detection (SPD) failure	Major
85E9	DIMM_N3 encountered a Serial Presence Detection (SPD) failure	Major
85EA	DIMM_O1 encountered a Serial Presence Detection (SPD) failure	Major
85EB	DIMM_O2 encountered a Serial Presence Detection (SPD) failure	Major
85EC	DIMM_O3 encountered a Serial Presence Detection (SPD) failure	Major

Error Code	Error Message	Response
85ED	DIMM_P1 encountered a Serial Presence Detection (SPD) failure	Major
85EE	DIMM_P2 encountered a Serial Presence Detection (SPD) failure	Major
85EF	DIMM_P3 encountered a Serial Presence Detection (SPD) failure	Major
8604	POST Reclaim of non-critical NVRAM variables	Minor
8605	BIOS Settings are corrupted	Major
8606	NVRAM variable space was corrupted and has been reinitialized	Major
92A3	Serial port component was not detected	Major
92A9	Serial port component encountered a resource conflict error	Major
A000	TPM device not detected.	Minor
A001	TPM device missing or not responding.	Minor
A002	TPM device failure.	Minor
A003	TPM device failed self test.	Minor
A100	BIOS ACM Error	Major
A421	PCI component encountered a SERR error	Fatal
A5A0	PCI Express* component encountered a PERR error	Minor
A5A1	PCI Express* component encountered an SERR error	Fatal
A6A0	DXE Boot Services driver: Not enough memory available to shadow a Legacy Option ROM.	Minor

POST Error Beep Codes

The following table lists the POST error beep codes. Prior to system video initialization, the BIOS uses these beep codes to inform users on error conditions. The beep code is followed by a user-visible code on the POST Progress LEDs

Table 86. POST Error Beep Codes

Beeps	Error Message	POST Progress Code	Description
1	USB device action	NA	Short beep sounded whenever a USB device is discovered in POST, or inserted or removed during runtime
1 long	Intel® TXT security violation	0xAE, 0xAF	System halted because Intel® Trusted Execution Technology detected a potential violation of system security.
3	Memory error	See Tables 28 and 29	System halted because a fatal error related to the memory was detected.
2	BIOS Recovery started	NA	Recovery boot has been initiated
4	BIOS Recovery failure	NA	BIOS recovery has failed. This typically happens so quickly after recovery us initiated that it sounds like a 2-4 beep code.

The Integrated BMC may generate beep codes upon detection of failure conditions. Beep codes are sounded each time the problem is discovered, such as on each power-up attempt, but are not sounded continuously. Codes that are common across all Intel server boards and systems that use same generation chipset are listed in the following table. Each digit in the code is represented by a sequence of beeps whose count is equal to the digit.

Table 87. Integrated BMC Beep Codes

Code	Reason for Beep	Associated Sensors
1-5-2-1	No CPUs installed or first CPU socket is empty.	CPU1 socket is empty, or sockets are populated incorrectly CPU1 must be populated before CPU2.
1-5-2-4	MSID Mismatch	MSID mismatch occurs if a processor is installed into a system board that has incompatible power capabilities.
1-5-4-2	Power fault	DC power unexpectedly lost (power good dropout) – Power unit sensors report power unit failure offset
1-5-4-4	Power control fault (power good assertion timeout).	Power good assertion timeout – Power unit sensors report soft power control failure offset
1-5-1-2	VR Watchdog Timer sensor assertion	VR controller DC power on sequence was not completed in time.
1-5-1-4	Power Supply Status	The system does not power on or unexpectedly powers off and a Power Supply Unit (PSU) is present that is an incompatible model with one or more other PSUs in the system.

Glossary

This appendix contains important terms used in the preceding chapters. For ease of use, numeric entries are listed first (for example,82460GX) with alpha entries following (for example, AGP 4x). Acronyms are then entered in their respective place, with non-acronyms following.

Term	Definition
ACPI	Advanced Configuration and Power Interface
AP	Application Processor
APIC	Advanced Programmable Interrupt Control
ASIC	Application Specific Integrated Circuit
BIOS	Basic Input/Output System
BIST	Built-In Self Test
BMC	Baseboard Management Controller
Bridge	Circuitry connecting one computer bus to another, allowing an agent on one to access the other
BSP	Bootstrap Processor
byte	8-bit quantity.
CBC	Chassis Bridge Controller (A microcontroller connected to one or more other CBCs, together they bridge the IPMB buses of multiple chassis.
CEK	Common Enabling Kit
CHAP	Challenge Handshake Authentication Protocol
CMOS	In terms of this specification, this describes the PC-AT compatible region of battery-backed 128 bytes of memory, which normally resides on the server board.
DPC	Direct Platform Control
EEPROM	Electrically Erasable Programmable Read-Only Memory
EHCI	Enhanced Host Controller Interface
EMP	Emergency Management Port
EPS	External Product Specification
FMB	Flexible Mother Board
FMC	Flex Management Connector
FMM	Flex Management Module
FRB	Fault Resilient Booting
FRU	Field Replaceable Unit
FSB	Front Side Bus
GB	1024MB
GPIO	General Purpose I/O
GTL	Gunning Transceiver Logic
HSC	Hot-Swap Controller
Hz	Hertz (1 cycle/second)
I2C	Inter-Integrated Circuit Bus
IA	Intel® Architecture
IBF	Input Buffer
ICH	I/O Controller Hub
ICMB	Intelligent Chassis Management Bus
IERR	Internal Error
IFB	I/O and Firmware Bridge

Term	Definition
INTR	Interrupt
IP	Internet Protocol
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
IR	Infrared
ITP	In-Target Probe
KB	1024 bytes
KCS	Keyboard Controller Style
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LPC	Low Pin Count
LUN	Logical Unit Number
MAC	Media Access Control
MB	1024KB
mBMC	National Semiconductor© PC87431x mini BMC
MCH	Memory Controller Hub
MD2	Message Digest 2 – Hashing Algorithm
MD5	Message Digest 5 – Hashing Algorithm – Higher Security
ms	milliseconds
MTTR	Memory Tpe Range Register
Mux	Multiplexor
NIC	Network Interface Controller
NMI	Nonmaskable Interrupt
OBF	Output Buffer
OEM	Original Equipment Manufacturer
Ohm	Unit of electrical resistance
PEF	Platform Event Filtering
PEP	Platform Event Paging
PIA	Platform Information Area (This feature configures the firmware for the platform hardware)
PLD	Programmable Logic Device
PMI	Platform Management Interrupt
POST	Power-On Self Test
PSMI	Power Supply Management Interface
PWM	Pulse-Width Modulation
RAM	Random Access Memory
RASUM	Reliability, Availability, Serviceability, Usability, and Manageability
RISC	Reduced Instruction Set Computing
ROM	Read Only Memory
RTC	Real-Time Clock (Component of ICH peripheral chip on the server board)
SDR	Sensor Data Record
SECC	Single Edge Connector Cartridge
SEEPROM	Serial Electrically Erasable Programmable Read-Only Memory
SEL	System Event Log
SIO	Server Input/Output

Term	Definition
SMI	Server Management Interrupt (SMI is the highest priority nonmaskable interrupt)
SMM	Server Management Mode
SMS	Server Management Software
SNMP	Simple Network Management Protocol
TBD	To Be Determined
TIM	Thermal Interface Material
UART	Universal Asynchronous Receiver/Transmitter
UDP	User Datagram Protocol
UHCI	Universal Host Controller Interface
UTC	Universal time coordinare
VID	Voltage Identification
VRD	Voltage Regulator Down
Word	16-bit quantity
ZIF	Zero Insertion Force

Reference Documents

See the following document for additional information:

- *BIOS for EPSD Platforms Based on Intel® Xeon Processor E5-4600/2600/2400/1600 Product Families External Product Specification*
- *EPSD Platforms Based On Intel Xeon® Processor E5 4600/2600/2400/1600 Product*
- *Families BMC Core Firmware External Product Specification*
- *Intel® Server System P4000IP/CR Technical Product Specification*
- *Intel® Server System R2000IP Technical Product Specification*
- *Intel® Remote Management Module 4 Technical Product Specification*
- *Intelligent Platform Management Interface Specification*
- *SmaRT and CLST Architecture on "Romley" Systems and Power Supplies Specification (Doc Reference # 461024)*
- *Intel Integrated RAID Module RMS25PB080, RMS25PB040, RMS25CB080, and RMS25CB040 Hardware Users Guide*