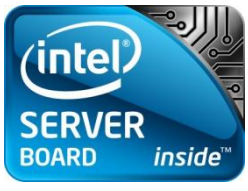
Intel® Server Boards S5520HC, S5500HCV, and S5520HCT

Technical Product Specification

Intel order number E39529-013



Revision 1.9

June 2011

Enterprise Platforms and Services Division

Revision History

Date	Revision Number	Modifications
February 2008	0.1	Preliminary Draft
March 2008	0.3	Content Update
March 2008	0.5	Updated sections 2.1 and 3.2
April 2008	0.55	Updated product code and processor support related information.
August 2008	0.6	Updated product code and memory support related information; S5500HCV DIMM slot population change; and Chassis Intrusion header location change
September 2008	0.65	Jumper block location change.
February 2009	1.0	Updated Block Diagram; Updated Functional Architecture Section; added BIOS Setup Utility Section; and updated Appendix.
March 2009	1.1	– Updated Section 3.3.4.1 Memory Reservation for Memory-mapped Functions – Updated Section 3.4.1.2 onboard SATA Storage Mode Matrix table – Added Fan Domain Table in Section 4.3.2.2.1 – Updated Section 9.2 MTBF – Added Appendix G Installation Guidelines – Added Processor Stepping Mismatching on Table 2 – Updated Boot Option BIOS Setup Menu (Table 34 and Figure 36) – Updated Table 4 Memory Running Frequency – Updated Table 12 Intel® SAS Entry RAID Module AXX4SASMOD Storage Mode – Updated Table 47 and Table 48, CPU 1 and CPU2 power connectors pin-out – Updated Table 84 POST Codes and Messages – Updated Table 87 BMC Beep Codes – Updated Figure 21 SMBUS Block Diagram, revised components code name – Updated Figure 53 Power Distribution Block Diagram, revised components code name
July 2009	1.2	– Updated Section 2.1, the feature set table – Updated Section 3.3.2 supported memory – Updated Section 3.3.3 – Added Section 3.15 – Updated Appendix A: adding PCI device SEL event decoding tips – Updated Appendix G – Updated Section 4.2.2 Keyboard, Video, and Mouse (KVM) Redirection – Updated Table 2, Table 8, Table 9, Table 25, Figure 13, and Figure 14
August 2009	1.3	Updated Section 3.15 and 7.3
November 2009	1.4	– Updated Section 3.3.3 – Updated Section 3.3.9 supported memory population
January 2010	1.5	– Updated Section 2.1, added security feature for S5520HCT – Added Section 3.13 Trusted Platform Module
March 2010	1.6	– Updated Section 2.1, added Intel® Xeon® Processor 5600 series support – Updated Section 3.2, added Intel® Xeon® Processor 5600 series support
April 2010	1.7	– Removed CCC related notices
May 2010	1.8	- Added Section 3.13.3 Intel® Trusted Execution Technology(Intel® TXT) - Update section 3.3.2 memory capacity
June 2011	1.9	- Update section 10.3 RRL KCC(Korea)

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, life saving, 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.

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Refer to the Intel® Server Boards S5520HC, S5500HCV and S5520HCT Specification Update for published errata.

Intel Corporation server baseboards 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 air flow required for their specific application and environmental conditions. Intel Corporation can not be held responsible if components fail or the server board does not operate correctly when used outside any of their published operating or non-operating limits.

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 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 Boards S5520HC, S5500HCV and S5520HCT.

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 – Overview
- Chapter 3 – Functional Architecture
- Chapter 4 – Platform Management
- Chapter 5 – BIOS Setup Utility
- Chapter 6 – Connector/Header Locations and Pin-outs
- Chapter 7 – Jumper Blocks
- Chapter 8 – Intel® Light Guided Diagnostics
- Chapter 9 – Design and Environmental Specifications
- Chapter 10 – Regulatory and Certification Information
- Appendix A – Integration and Usage Tips
- Appendix B – Compatible Intel® Server Chassis
- Appendix C – BMC Sensor Tables
- Appendix D – Platform Specific BMC Appendix
- Appendix E – POST Code Diagnostic LED Decoder
- Appendix F – POST Error Messages and Handling
- Appendix G – Installation Guidelines
- 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. Overview

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT are monolithic printed circuit boards (PCBs) with features designed to support the pedestal server markets.

2.1 Intel® Server Boards S5520HC, S5500HCV and S5520HCT Feature Set

Feature	Description
Processors	• Support for one or two Intel® Xeon® Processor(s) 5500 series up to 95W Thermal Design Power • Support for one or two Intel® Xeon® Processor(s) 5600 series up to 130W Thermal Design Power • 4.8 GT/s, 5.86 GT/s, and 6.4 GT/s Intel® QuickPath Interconnect (Intel® QPI) • FC-LGA 1366 Socket B ▪ Enterprise Voltage Regulator-Down (EVRD) 11.1
Memory	• Six memory channels (three channels for each processor socket) ▪ Channels A, B, C, D, E, and F • Support for 800/1066/1333 MT/s ECC Registered DDR3 Memory (RDIMM), ECC Unbuffered DDR3 memory ((UDIMM) • No support for mixing of RDIMMs and UDIMMs • Intel® Server Board S5520HC/S5520HCT: ▪ 12 DIMM slots ▪ Two DIMM slots per channel • Intel® Server Board S5500HCV ▪ Nine DIMM slots ▪ Two DIMM slots on Channels A, B, and C ▪ One DIMM slot on Channels D, E, and F
Chipset	• Intel® Server Board S5520HC/S5520HCT: ▪ Intel® 5520 Chipset ▪ Intel® 82801JIR I/O Controller Hub (ICH10R) • Intel® Server Board S5500HCV: ▪ Intel® 5500 Chipset ▪ Intel® 82801JIR I/O Controller Hub (ICH10R)
Cooling Fan Support	Support for • Two processor fans (4-pin headers) • Four front system fans (6-pin headers) • One rear system fans (4-pin header) • 3-pin fans are compatible with all fan headers

Feature	Description
Add-in Card Slots	• Intel® Server Board S5520HC/S5520HCT: Six expansion slots ▪ One full-length/full-height PCI Express* Gen2 slot (x16 Mechanically, x8 Electrically) ▪ Three full-length/full-height PCI Express* Gen2 x8 slots ▪ One full-length/full-height PCI Express* Gen1 slot (x8 Mechanically, x4 Electrically) shared with SAS Module slot*. ▪ One 32-bit/33 MHz PCI slot, keying for 5-V and Universal PCI add-in card • Intel® Server Board S5500HCV: Five expansion slots ▪ One full-length/full-height PCI Express* Gen2 slot (x16 Mechanically, x4 Electrically) ▪ Two full-length/full-height PCI Express* Express* Gen2 x8 slots ▪ One full-length/full-height PCI Express* Gen1 slot (x8 Mechanically, x4 Electrically) shared with SAS Module slot*. ▪ One 32-bit/33 MHz PCI slot, keying for 5-volt and Universal PCI add-in card
Hard Drive and Optical Drive Support	• Optical devices are supported • Six SATA connectors at 1.5 Gbps and 3 Gbps • Four SAS connectors at 3 Gbps through optional Intel® SAS Entry RAID Module AXX4SASMOD
RAID Support	• Intel® Embedded Server RAID Technology II through onboard SATA connectors provides SATA RAID 0, 1, and 10 with optional RAID 5 support provided by the Intel® RAID Activation Key AXXRAKSW5 • Intel® Embedded Server RAID Technology II through optional Intel® SAS Entry RAID Module AXX4SASMOD provides SAS RAID 0, 1, and 10 with optional RAID 5 support provided by the Intel® RAID Activation Key AXXRAKSW5 • IT/IR RAID through optional Intel® SAS Entry RAID Module AXX4SASMOD provides entry-level hardware RAID 0, 1, 10/10E, and native SAS pass through mode • 4 ports full featured SAS/SATA hardware RAID through optional Intel® Integrated RAID Module SROMBSASMR (AXXROMBSASMR), provides RAID 0, 1, 5, 6 and striping capability for spans 10, 50, 60.
USB Drive Support	• One internal type A USB port with USB 2.0 support that supports a peripheral, such as a floppy drive • One internal low-profile USB port for USB Solid State Drive
I/O control support	• External connections: ▪ DB9 serial port A connection ▪ One DH 10 serial port connector (optional) ▪ Two RJ-45 NIC connectors for 10/100/1000 Mb connections: Dual GbE through the Intel® 82575EB Network Connection. ▪ Four USB 2.0 ports at the back of the board • Internal connections: ▪ Two 9-pin USB headers, each supports two USB 2.0 ports ▪ One DH10 serial port B header ▪ Six SATA connectors at 1.5 Gbps and 3 Gbps ▪ Four SAS connectors at 3 Gbps (optional) ▪ One SSI-compliant 24-pin front control panel header
Video Support	• ServerEngines* LLC Pilot II* with 64 MB DDR2 memory, 8 MB allocated to graphics ▪ Integrated 2D video controller ▪ Dual monitor video mode is supported
LAN	• Two Gigabit through Intel® 82575EB PHYs with Intel® I/O Acceleration Technology 2 support
Security**	• Trusted Platform Module

Feature	Description
Server Management	• Onboard ServerEngines* LLC Pilot II* Controller ▪ Integrated Baseboard Management Controller (Integrated BMC), IPMI 2.0 compliant ▪ Integrated Super I/O on LPC interface • Support for Intel® Remote Management Module 3 • Intel® Light-Guided Diagnostics on field replaceable units • Support for Intel® System Management Software 3.1 and beyond • Support for Intel® Intelligent Power Node Manager (Need PMBus-compliant power supply)
BIOS Flash	• Winbond* W25X64
Form Factor	• SSI EEB (12”x13”)
Compatible Intel® Server Chassis	• Intel® Server Chassis SC5650DP • Intel® Server Chassis SC5650BRP (PMBus-compliant Power Supply) • Intel® Server Chassis SC5600Base • Intel® Server Chassis SC5600BRP (PMBus-compliant Power Supply) • Intel® Server Chassis SC5600LX (PMBus-compliant Power Supply)

* The PCI Express* Gen 1 slot (x8 Mechanically, x4 Electrically) is not available when the SAS module slot is in use and vice versa.

**The Trusted Platform Module is only availabe in S5520HCT

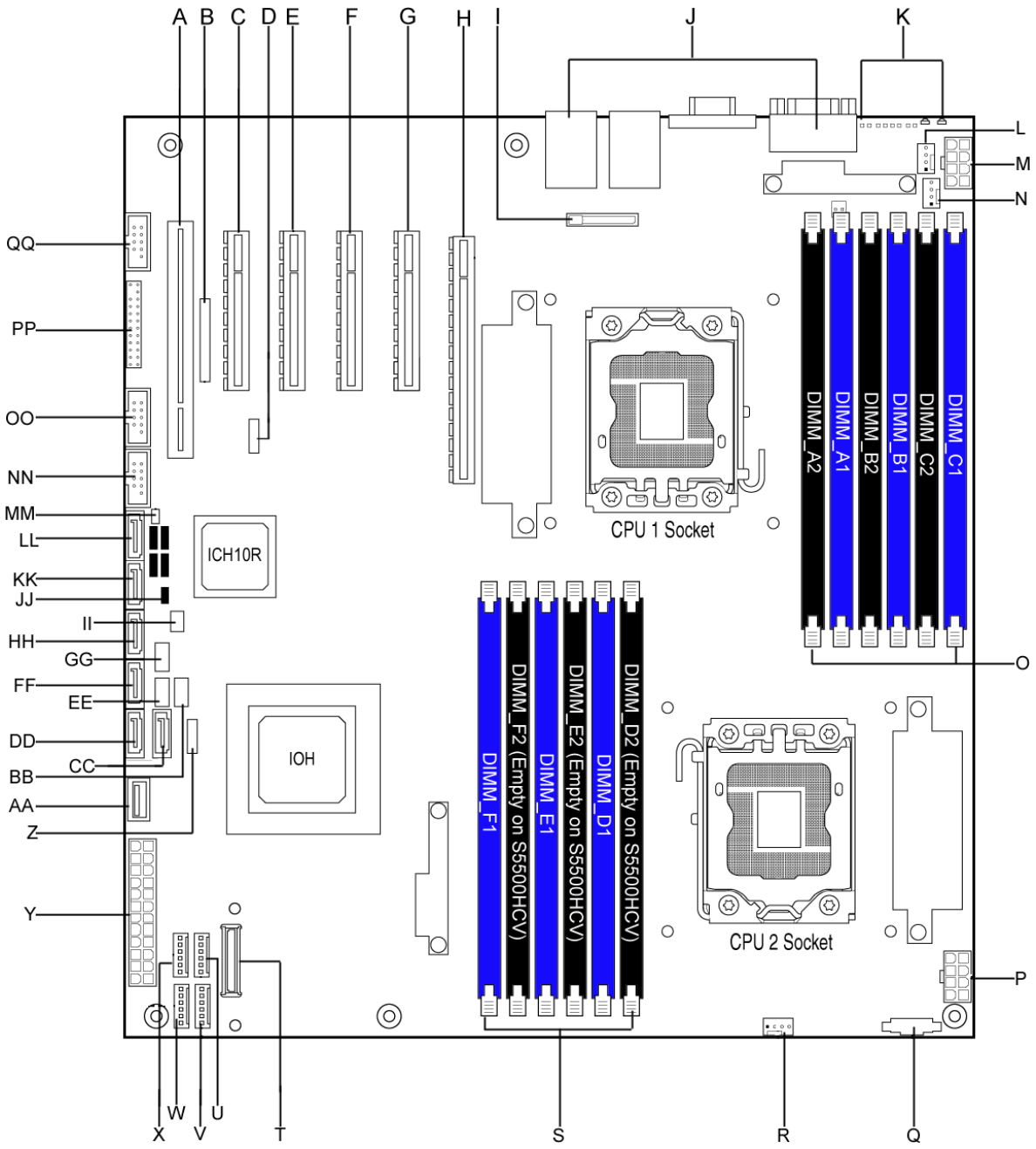
Server Board Layout

Figure 1. Intel® Server Board S5520HC

Figure 2. Intel® Server Board S5500HCV

2.1.1 Server 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, 32-bit/33 MHz PCI, Keying for 5V and Universal	W	System Fan 2 Header (6-pin)
B	Intel® RMM3 Slot	X	System Fan 1 Header (6-pin)
C	Slot 2, PCI Express* x4 (x8 Mechanically)	Y	Main Power Connector
D	Low-profile USB Solid State Drive Header	Z	LCP/IPMB Header
E	Slot 3, PCI Express* Gen2 x8	AA	Type A USB Port
F	Slot 4, PCI Express* Gen2 x8	BB	SATA SGPIO Header
G	Slot 5, PCI Express* Gen2 x8 (Empty on Intel® Server Board S5500HCV)	CC	SATA Port 0
H	S5520HC: Slot 6, PCI Express* Gen2 x8 (x16	DD	SATA Port 1

Callout	Description	Callout	Description
	Mechanically) S5500HCV: Slot 6, PCI Express* Gen2 x4 (x16 Mechanically)		
I	Battery	EE	HSBP_B
J	Back Panel I/O Ports	FF	SATA Port 2
K	Diagnostic and Identify LED's	GG	HSBP_A
L	System Fan 5 Header (4-pin)	HH	SATA Port 3
M	Power Connector for Processor 1 and Memory attached to Processor 1	II	SATA Software RAID 5 Key Header
N	Processor 1 Fan Header (4-pin)	JJ	Chassis Intrusion Header
O	DIMM Sockets of Memory Channel A, B, and C	KK	SATA Port 4
P	Power Connector for Processor 2 and Memory attached to Processor 2	LL	SATA Port 5
Q	Auxiliary Power Signal Connector	MM	HDD Activity LED Header (Connect to Add-in Card HDD Activity LED Header)
R	Processor 2 Fan Header (4-pin)	NN	USB Connector (9-pin, for front panel USB ports)
S	DIMM Sockets of Memory Channel D, E, and F	OO	USB Connector (9-pin)
T	SAS Module Slot	PP	Front Control Panel header
U	System Fan 3 Header (6-pin)	QQ	DH-10 Serial B header
V	System Fan 4 Header (6-pin)		

Figure 3. Major Board Components

2.1.2 Server Board Mechanical Drawings

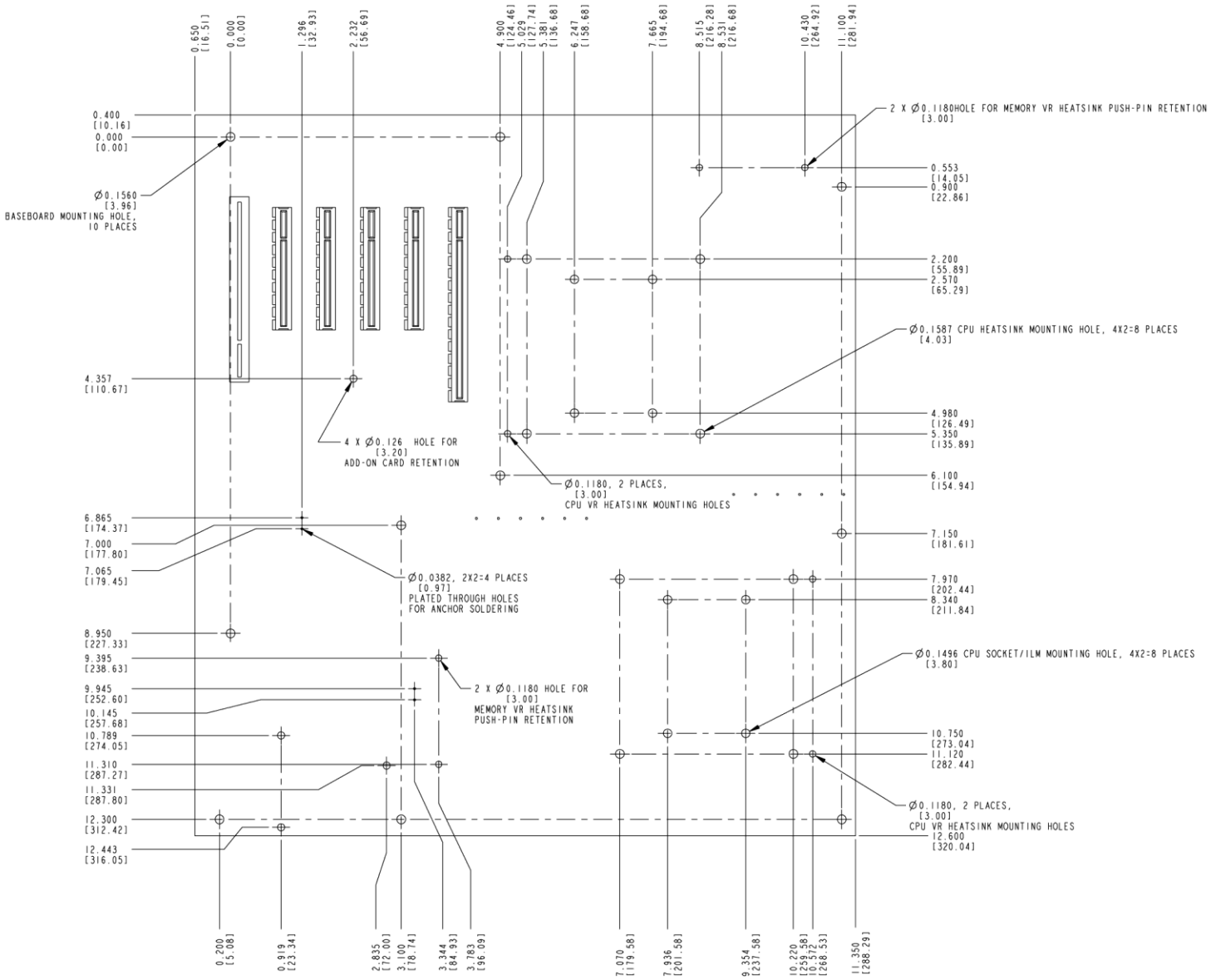


Figure 4. Mounting Hole Locations

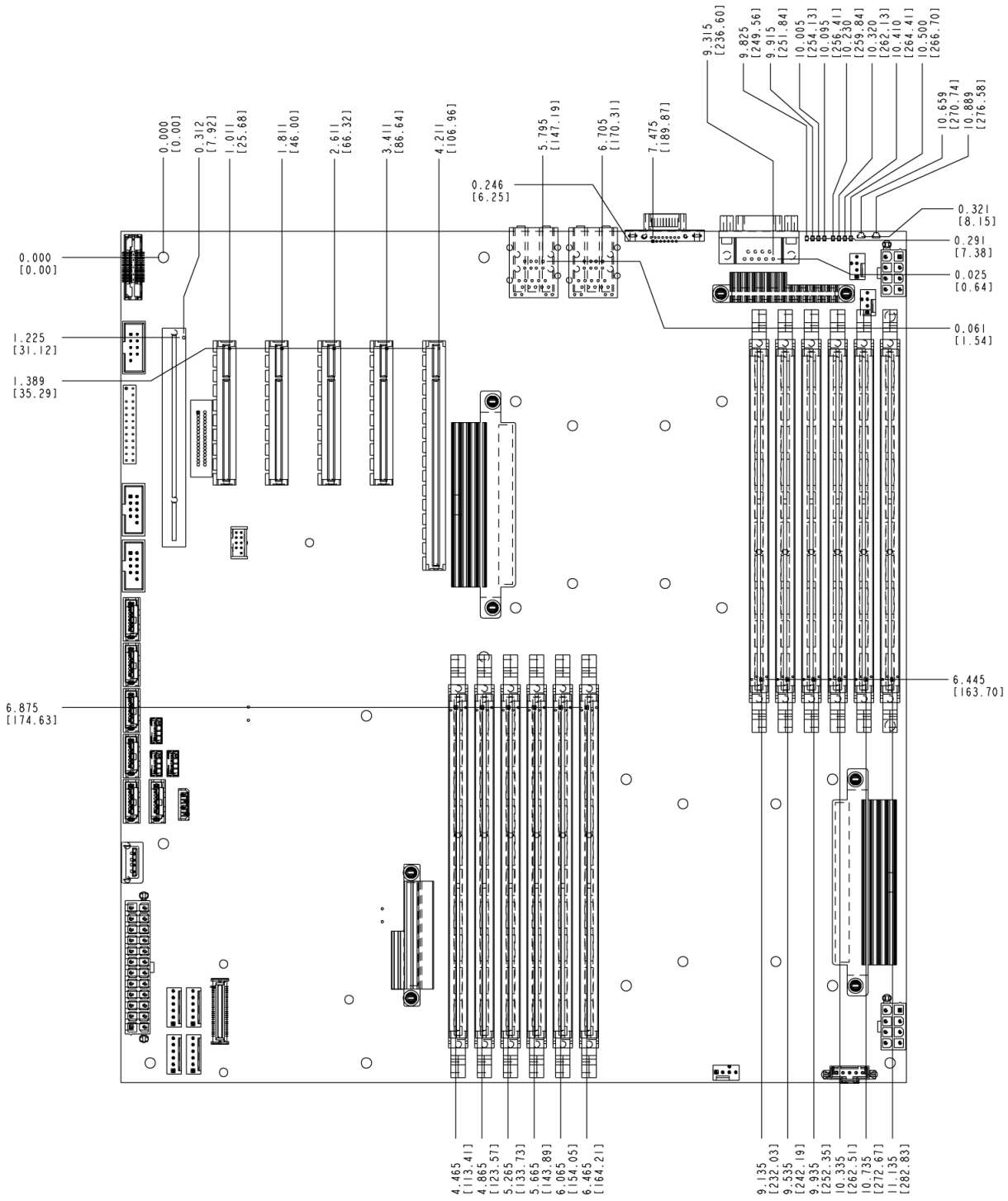


Figure 5. Major Connector Pin-1 Locations (1 of 2)

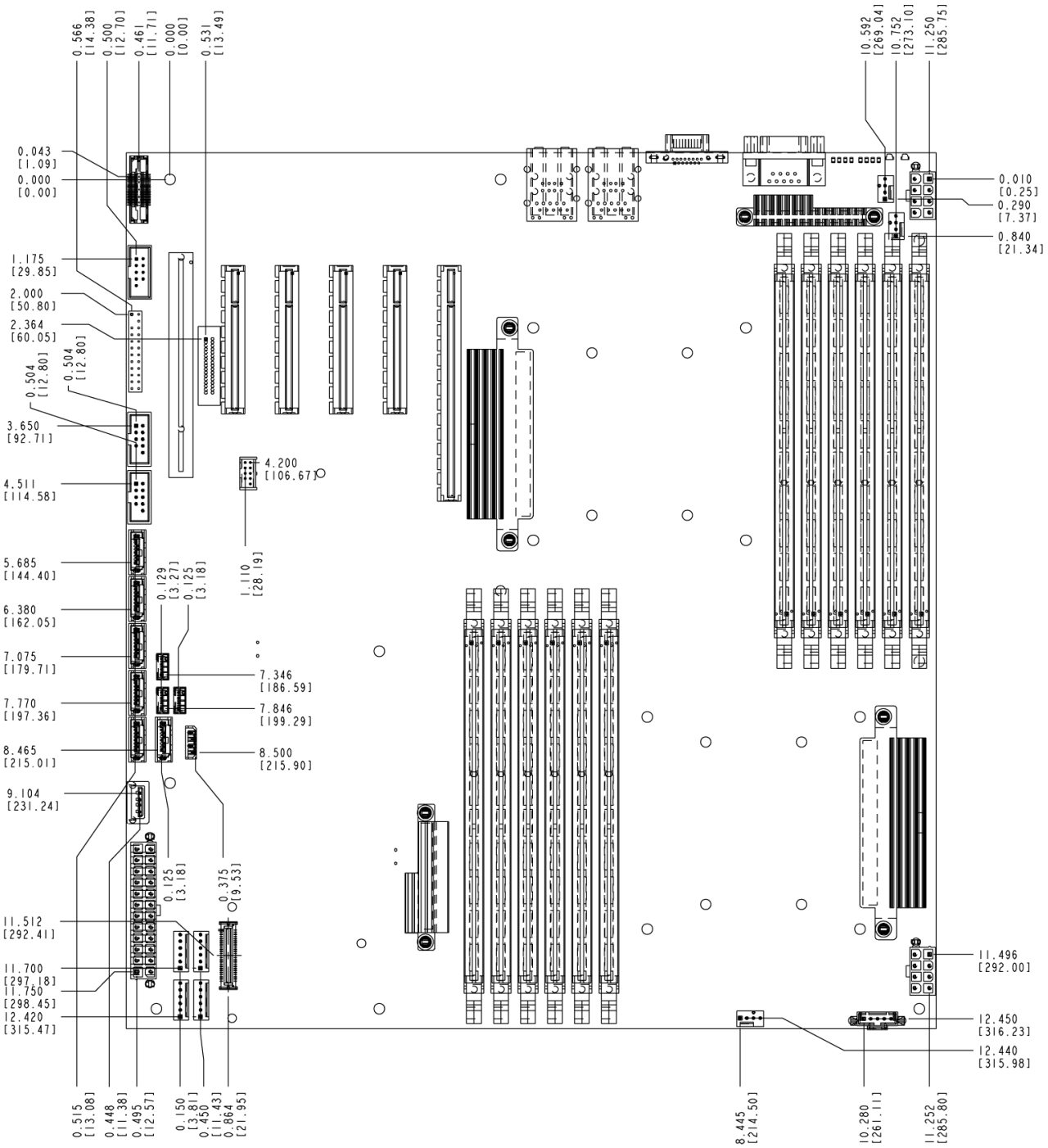


Figure 6. Major Connector Pin-1 Locations (2 of 2)

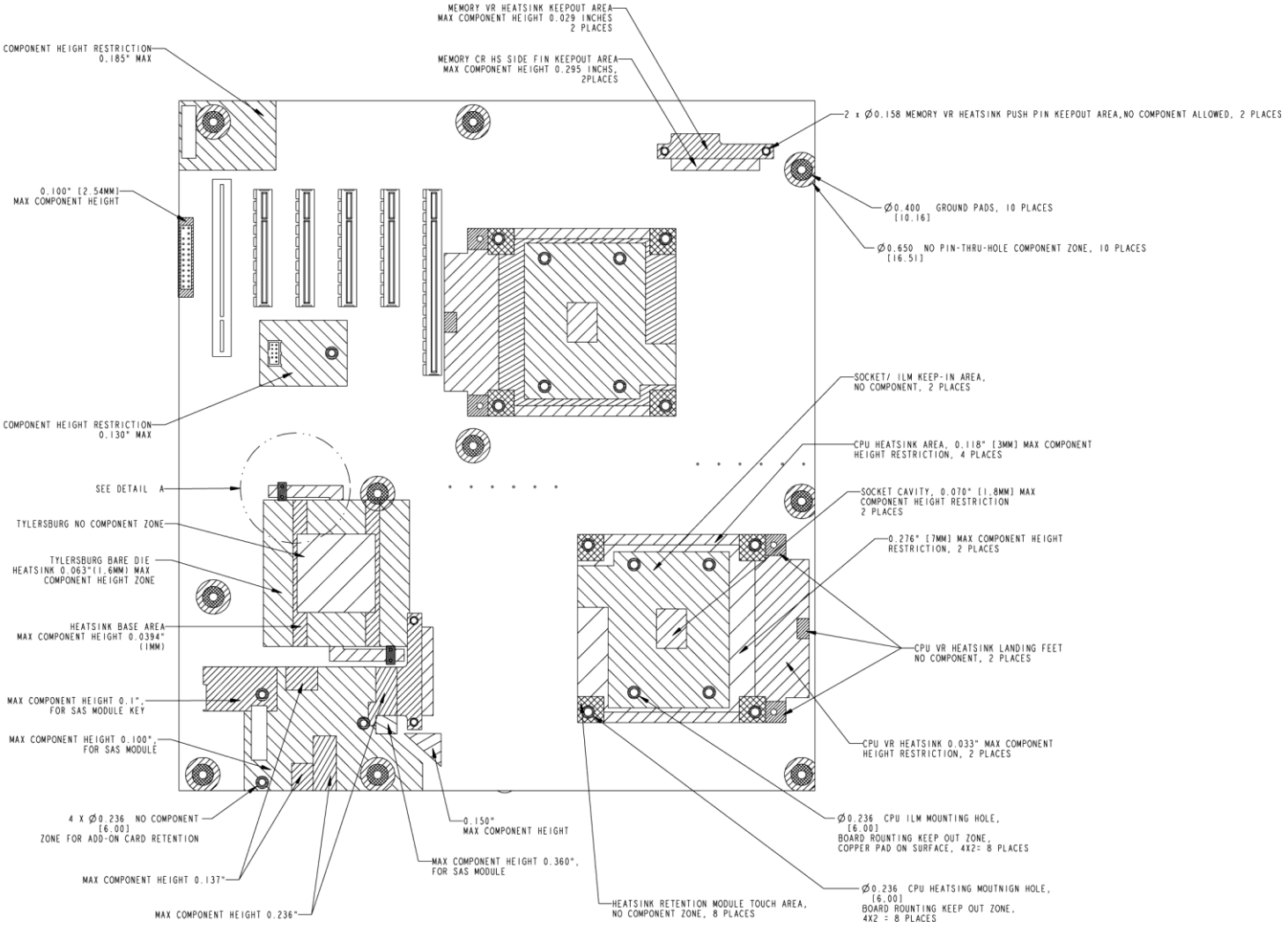


Figure 7. Primary Side Keep-out Zone (1 of 2)

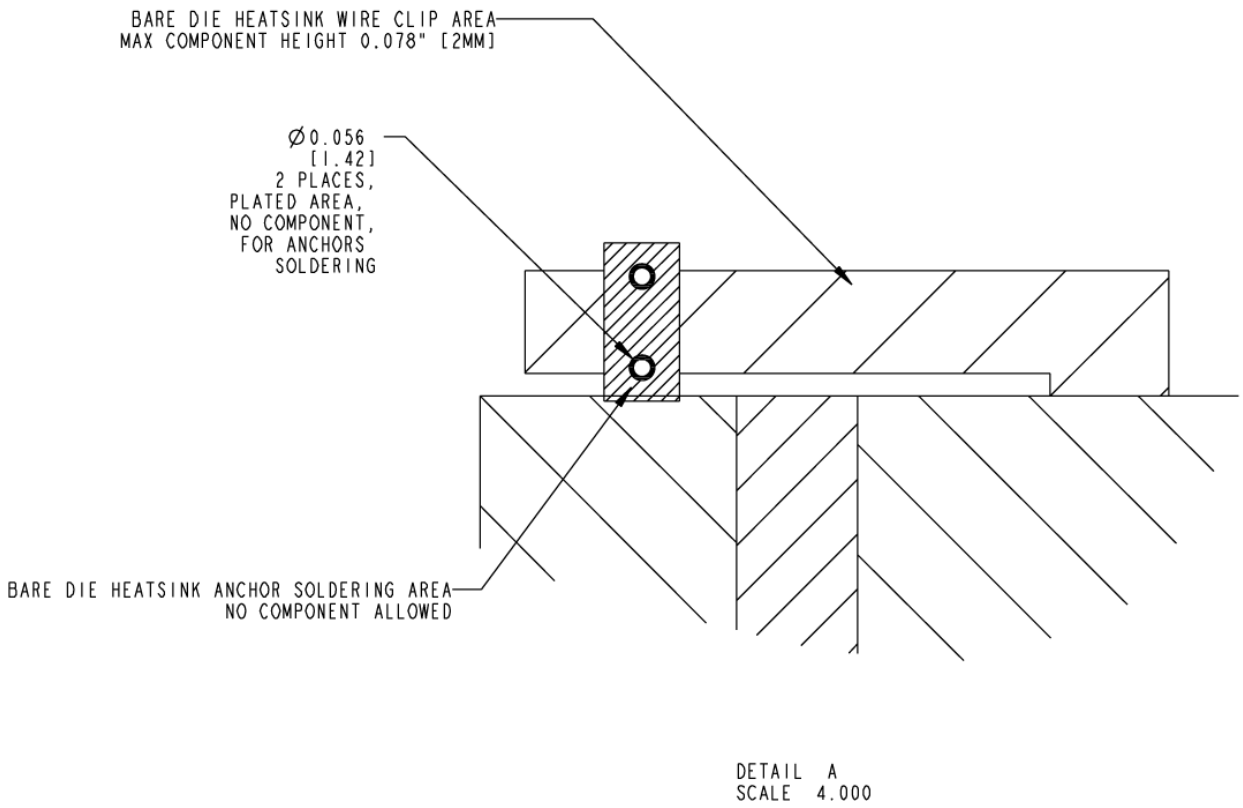


Figure 8. Primary Side Keep-out Zone (2 of 2)

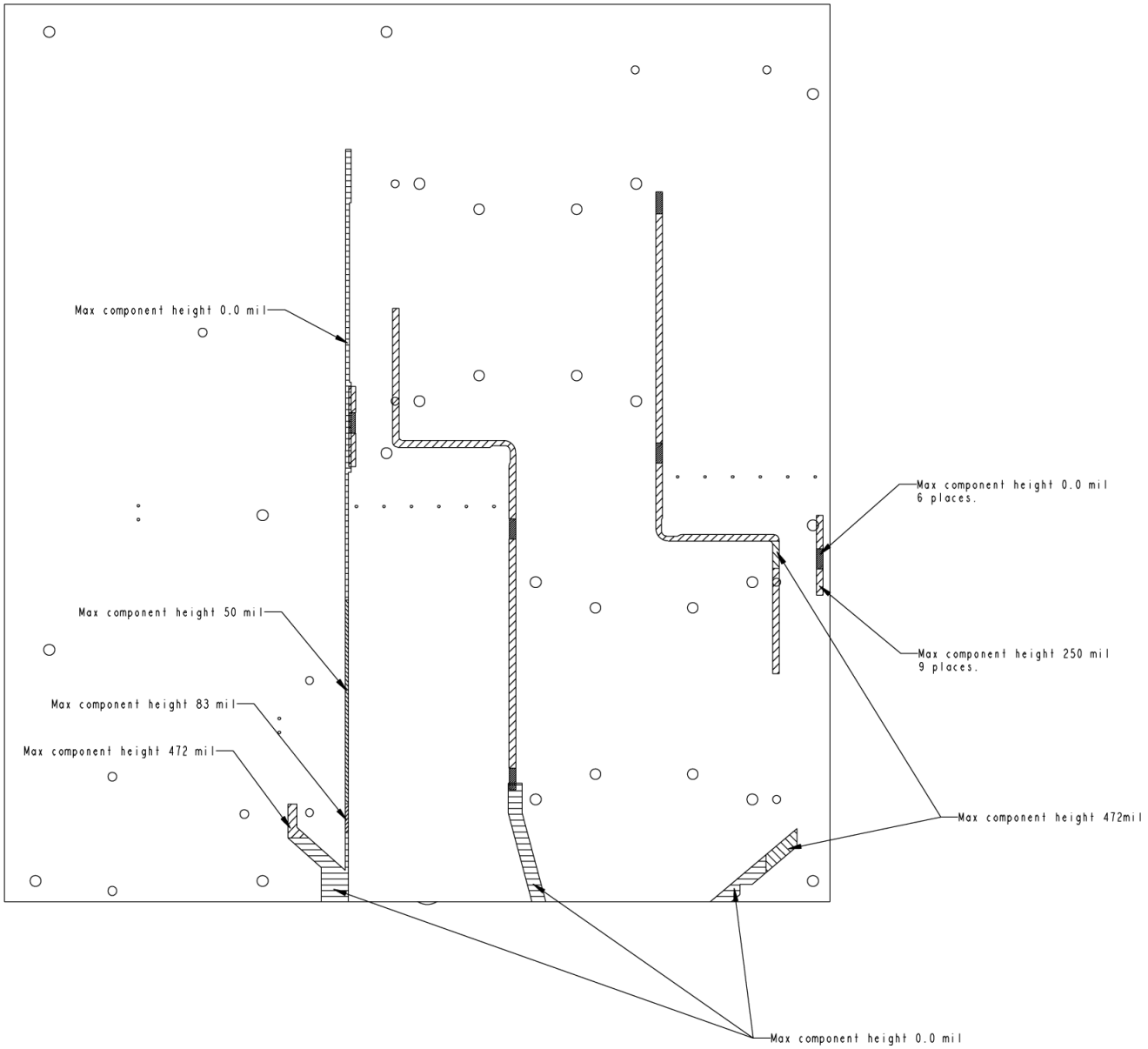


Figure 9. Primary Side Air Duct Keep-out Zone

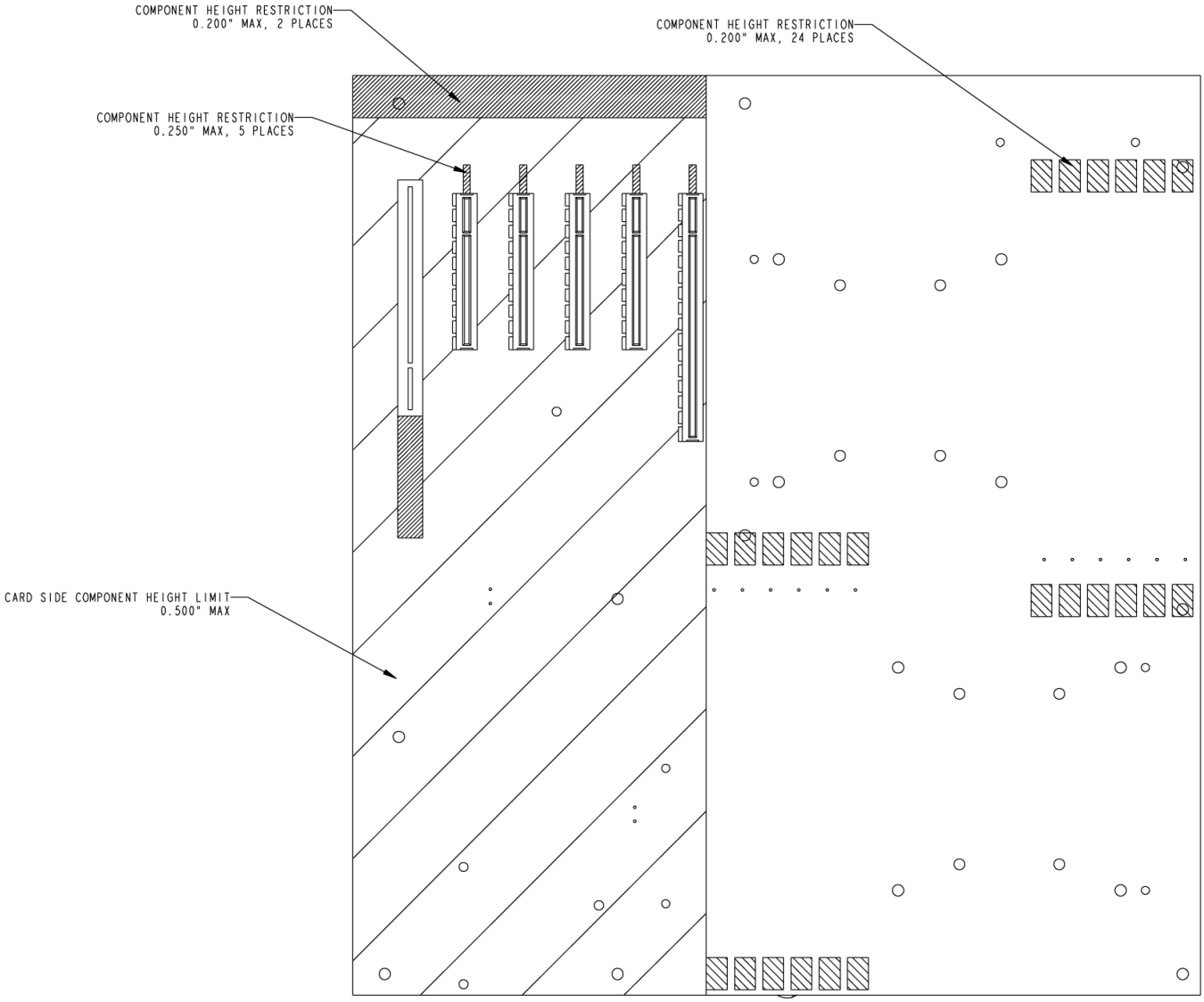


Figure 10. Primary Side Card-Side Keep-out Zone

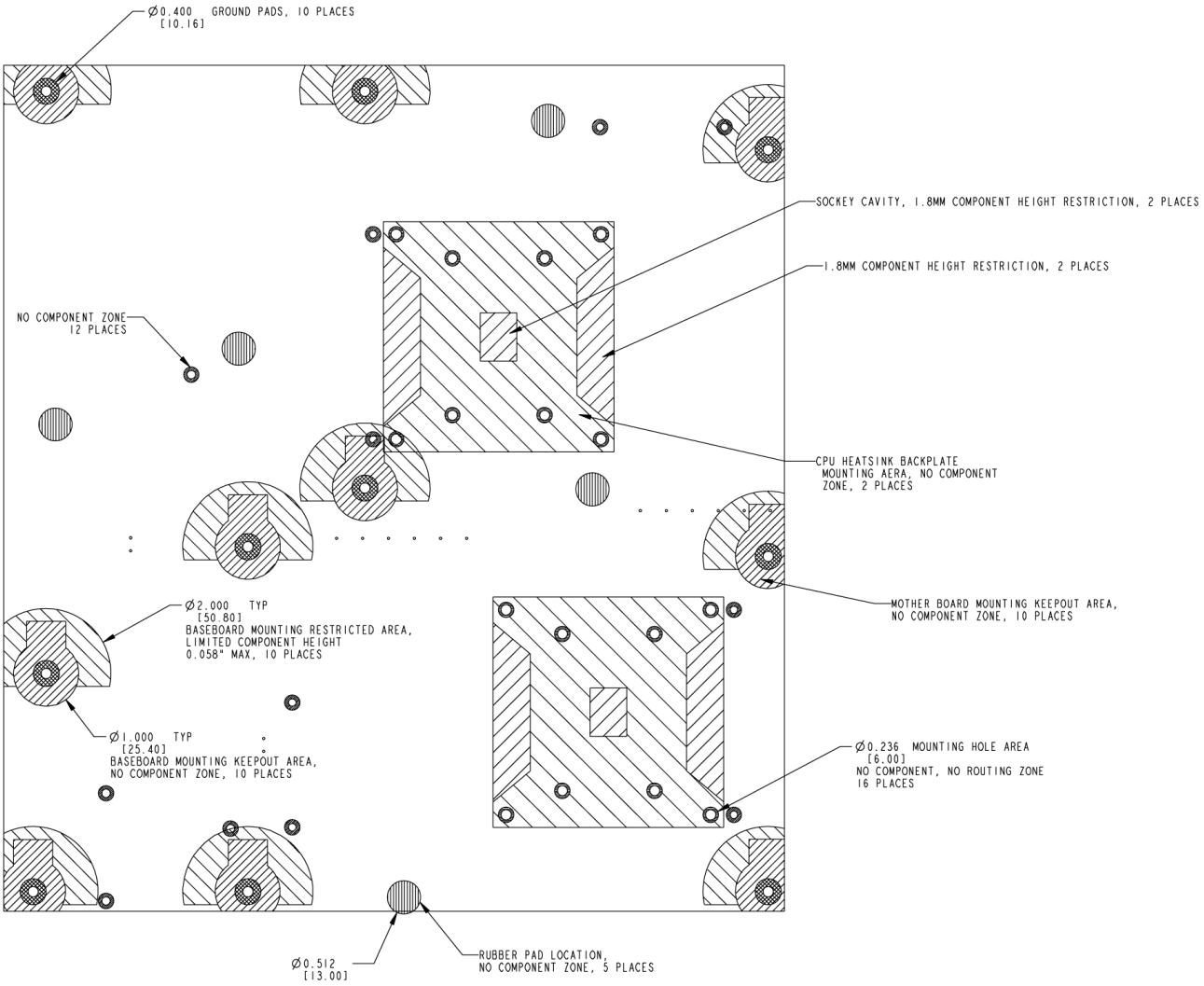
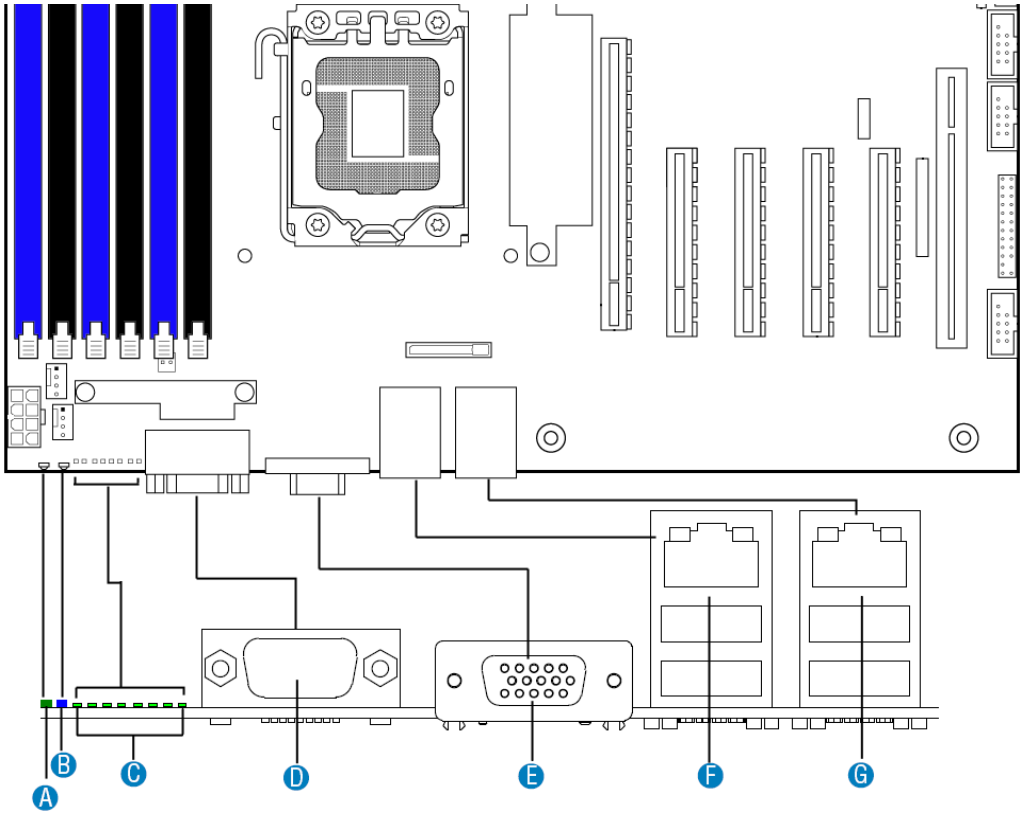


Figure 11. Second Side Keep-out Zone

2.1.3 Server 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	System Status LED	E	Video
B	ID LED	F	NIC Port 1 (1 Gb, Default Management Port) USB Port 2 (top), 3 (bottom)
C	Diagnostics LED's	G	NIC Port 2 (1 Gb) USB Port 0 (top), 1 (bottom)
D	Serial Port A		

Figure 12. Rear I/O Layout

3. Functional Architecture

The architecture and design of the Intel® Server Boards S5520HC, S5500HCV and S5520HCTis based on the Intel® 5520/5500 and ICH10R chipset. The chipset is designed for systems based on the Intel® Xeon® Processor 5500 Series in an FC-LGA 1366 Socket B package with Intel® QuickPath Interconnect (Intel® QPI) speed at 6.40 GT/s, 5.86 GT/s, and 4.80 GT/s.

The chipset contains two main components:

- Intel® 5520 I/O Hub or 5500 I/O Hub, which provides a connection point between various I/O components and the Intel® QuickPath Interconnect (Intel® QPI) based processors
- Intel® ICH10 RAID (ICH10R) I/O controller hub for the I/O subsystem

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.

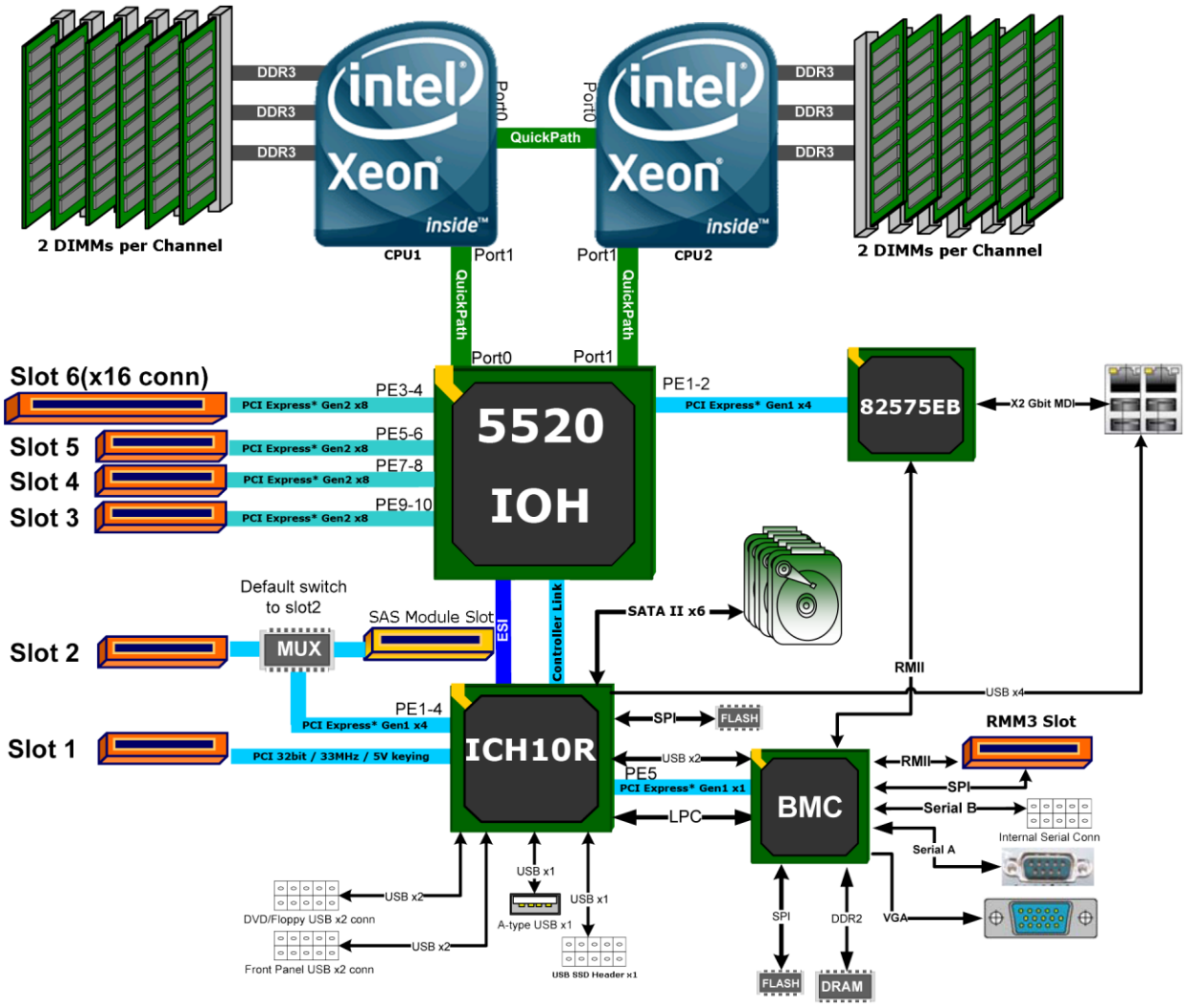


Figure 13. Intel® Server Board S5520HC Functional Block Diagram

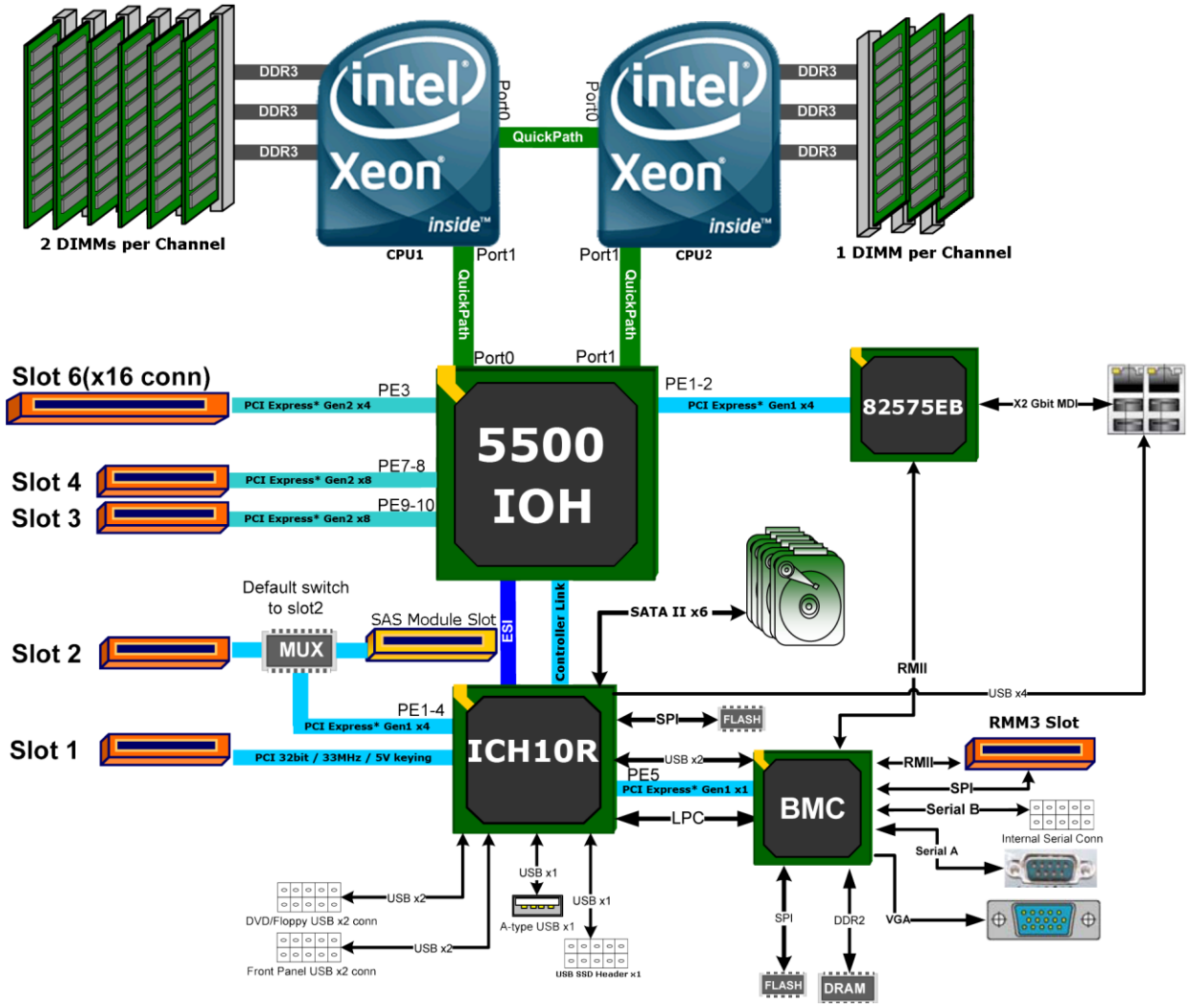


Figure 14. Intel® Server Board S5500HCV Functional Block Diagram

3.1 Intel® 5520 and 5500 I/O Hub (IOH)

The Intel® 5520 and 5500 I/O Hub (IOH) in the Intel® Server Boards S5520HC, S5500HCV and S5520HCT provide a connection point between various I/O components and Intel® QPI-based processors, which includes the following core platform functions:

- Intel® QPI link interface for the processor subsystem
- PCI Express* Ports
- Enterprise South Bridge Interface (ESI) for connecting Intel® ICH10R
- Manageability Engine (ME)
- Controller Link (CL)
- SMBus Interface
- Intel® Virtualization Technology for Directed I/O (Intel® VT-d)

The following table shows the high-level features of the Intel® 5520 and 5500 IOH:

Table 1. IOH High-Level Summary

IOH SKU	Intel® QPI Ports	Supported Processor	PCI Express* Lanes	Manageability
5520	2	Intel® Xeon® Processor 5500 Series	36	Intel® Intelligent Power Node Manager
5500	2	Intel® Xeon® Processor 5500 Series	24	Intel® Intelligent Power Node Manager

3.1.1 Intel® QuickPath Interconnect

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT provide two full-width, cache-coherent, link-based Intel® QuickPath Interconnect interfaces from Intel® 5520 and 5500 IOH for connecting Intel® QPI based processors. The two Intel® QPI link interfaces support full-width communication only and have the following main features:

- Packetized protocol with 18 data/protocol bits and 2 CRC bits per link per direction
  - Supporting 4.8 GT/s, 5.86 GT/s, and 6.4 GT/s
- Fully-coherent write cache with inbound write combining
- Read Current command support
- Support for 64-byte cache line size

3.1.2 PCI Express* Ports

The Intel® 5520 IOH is capable of interfacing with up to 36 PCI Express* Gen2 lanes, which support devices with the following link width: x16, x8, x4, x2, and x1.

The Intel® 5500 IOH is capable of interfacing with up to 24 PCI Express* Gen2 lanes, which support devices with the following link width: x16, x8, x4, x2, and x1.

All ports support PCI Express* Gen1 and Gen2 transfer rates.

For a detailed PCI Express* Slots definition in the Intel® Server Boards S5520HC, S5500HCV and S5520HCT, see “3.5 PCI Subsystem.”

3.1.3 Enterprise South Bridge Interface (ESI)

One x4 ESI link interface supporting PCI Express Gen1 (2.5 Gbps) transfer rate for connecting Intel® ICH10R in the Intel® Server Boards S5520HC, S5500HCV and S5520HCT.

3.1.4 Manageability Engine (ME)

An embedded ARC controller is within the IOH providing the Intel® Server Platform Services (SPS). The controller is also commonly referred to as the Manageability Engine (ME).

3.1.5 Controller Link (CL)

The Controller Link is a private, low-pin count (LPC), low power, communication interface between the IOH and the ICH10 portions of the Manageability Engine subsystem.

3.2 Processor Support

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT support the following processors:

- One or two Intel® Xeon® Processor 5500 Series with a 4.8 GT/s, 5.86 GT/s, or 6.4 GT/s Intel® QPI link interface and Thermal Design Power (TDP) up to 95 W.
- One or two Intel® Xeon® Processor 5600 Series with a 6.4 GT/s Intel® QPI link interface and Thermal Design Power (TDP) up to 130 W.

The server boards do not support previous generations of the Intel® Xeon® Processors.

For a complete updated list of supported processors, see: http://support.intel.com/support/motherboards/server/S5520HC/. On the Support tab, look for "Compatibility" and then "Supported Processor List".

3.2.1 Processor Population Rules

You must populate processors in sequential order. Therefore, you must populate Processor socket 1 (CPU 1) before processor socket 2 (CPU 2).

When only one processor is installed, it must be in the socket labeled CPU1, which is located near the rear edge of the server board. When a single processor is installed, no terminator is required in the second processor socket.

For optimum performance, when two processors are installed, both must be the identical revision and have the same core voltage and Intel® QPI/core speed.

3.2.2 Mixed Processor Configurations.

The following table describes mixed processor conditions and recommended actions for the Intel® Server Boards S5520HC, S5500HCV and S5520HCT. Errors fall into one of three categories:

- **Halt:** 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 if the "Post Error Pause" setup option is enabled or disabled. After entering setup, the error message displays on the Error Manager screen, and an error is logged to the System Event Log (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.
- **Pause:** If the "Post Error Pause" setup option is enabled, the system goes directly to the Error Manager screen to display the error and log the error code to SEL. Otherwise, the system continues to boot and no prompt is given for the error, although the 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. The system continues booting in a degraded state regardless of if the "Post Error Pause" setup option is enabled or disabled. The user may want to replace the erroneous unit.

Table 2. Mixed Processor Configurations

Error	Severity	System Action
Processor family not identical	Halt	The BIOS detects the error condition and responds as follows: – Logs the error into the system event log (SEL). – Alerts the Integrated BMC about the configuration error. – Does not disable the processor. – Displays “0194: Processor 0x family mismatch detected” message in the Error Manager. – Halts the system and will not boot until the fault condition is remedied.
Processor stepping mismatch	Pause	The BIOS detects the stepping difference and responds as follows: – Checks to see whether the steppings are compatible – typically +/- one stepping. – If so, no error is generated (this is not an error condition). – Continues to boot the system successfully. Otherwise, this is a stepping mismatch error, and the BIOS responds as follows: – Displays “0193: Processor 0x stepping mismatch” message in the Error Manager and logs it into the SEL. – Takes Minor Error action and continues to boot the system.
Processor cache not identical	Halt	The BIOS detects the error condition and responds as follows: – Logs the error into the SEL. – Alerts the Integrated BMC about the configuration error. – Does not disable the processor. – Displays “0192: Processor 0x cache size mismatch detected” message in the Error Manager. – Halts the system and will not boot until the fault condition is remedied.
Processor frequency (speed) not identical	Halt	The BIOS detects the error condition 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 the BIOS: – Logs the error into the SEL. – Displays “0197: Processor 0x family is not supported” message in the Error Manager. – Halts the system and will not boot until the fault condition is remedied.

Error	Severity	System Action
Processor Intel® QuickPath Interconnect speeds not identical	Halt	The BIOS detects the error condition and responds as follows: – Adjusts all processor QPI frequencies to highest common frequency. – No error is generated – this is not an error condition – Continues to boot the system successfully. If the link speeds for all QPI links cannot be adjusted to be the same, then the BIOS: – Logs the error into the SEL. – Displays "0195: Processor 0x Intel® QPI speed mismatch" message in the Error Manager. – Halts the system and will not boot until the fault condition is remedied.
Processor microcode missing	Minor	The BIOS detects the error condition and responds as follows: – Logs the error into the SEL. – Does not disable the processor. – Displays "8180: 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 Setup.

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

If the installed processor supports the Intel® Hyper-Threading Technology, the BIOS Setup provides an option to enable or disable this feature. The default is enabled.

The BIOS creates additional entries in the ACPI MP tables to describe the virtual processors. The SMBIOS Type 4 structure shows only the installed physical processors. It does not describe the virtual processors.

Because some operating systems are not able to efficiently use the Intel® HT Technology, the BIOS does not create entries in the Multi-Processor Specification, Version 1.4 tables to describe the virtual processors.

3.2.4 Enhanced Intel SpeedStep® Technology (EIST)

If the installed processor supports the Enhanced Intel SpeedStep® Technology, the BIOS Setup provides an option to enable or disable this feature. The Default is enabled.

3.2.5 Intel® Turbo Boost Technology

Intel® Turbo Boost Technology opportunistically and automatically allows the processor to run faster than the marked frequency if the part is operating below power, temperature, and current limits.

If the processor supports this feature, the BIOS setup provides an option to enable or disable this feature. The default is enabled.

3.2.6 Execute Disable Bit Feature

The Execute Disable Bit feature (XD bit) can prevent data pages from being used by malicious software to execute code. A processor with the XD bit feature can provide memory protection in one of the following modes:

- Legacy protected mode if Physical Address Extension (PAE) is enabled.

- Intel® 64 mode when 64-bit extension technology is enabled (Entering Intel® 64 mode requires enabling PAE).

You can enable and disable the XD bit in the BIOS Setup. The default behavior is enabled.

3.2.7 Core Multi-Processing

The BIOS setup provides the ability to selectively enable one or more cores. The default behavior is to enable all cores. You can do this through the BIOS setup option for active core count.

The BIOS creates entries in the Multi-Processor Specification, Version 1.4 tables to describe multi-core processors.

3.2.8 Direct Cache Access (DCA)

Direct Cache Access (DCA) is a system-level protocol in a multi-processor system to improve I/O network performance, thereby providing higher system performance. The basic idea is to minimize cache misses when a demand read is executed. This is accomplished by placing the data from the I/O devices directly into the processor cache through hints to the processor to perform a data pre-fetch and install it in its local caches.

The BIOS setup provides an option to enable or disable this feature. The default behavior is enabled.

3.2.9 Unified Retention System Support

The server boards comply with Unified Retention System (URS) and Unified Backplate Assembly. The server boards ship with Unified Backplate Assembly at each processor socket.

The URS retention transfers load to the server boards via the Unified Backplate Assembly. The URS spring, captive in the heatsink, provides the necessary compressive load for the thermal interface material (TIM). All components of the URS heatsink solution are captive to the heatsink and only require a Phillips* screwdriver to attach to the Unified Backplate Assembly. See the following figure for the stacking order of URS components.

The Unified Backplate Assembly is removable, allowing for the use of non-Intel® heatsink retention solutions.

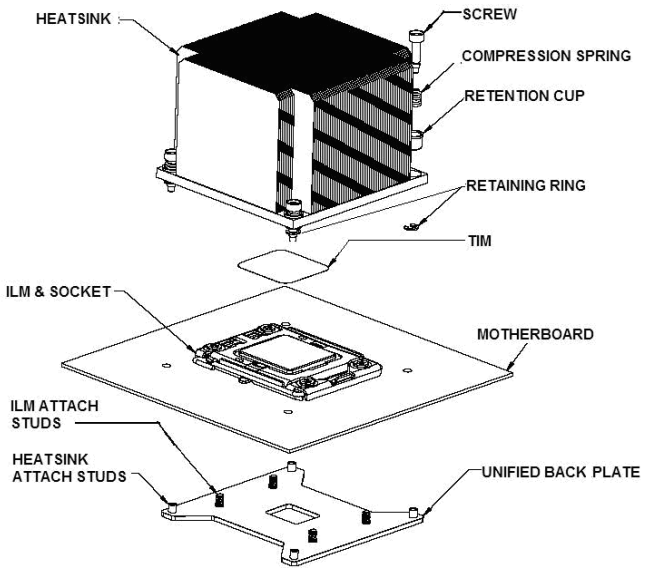


Figure 15. Unified Retention System and Unified Back Plate Assembly

3.3 Memory Subsystem

The Intel® Xeon® Processor 5500 Series on the Intel® Server Boards S5520HC, S5500HCV and S5520HCT are populated on CPU sockets. Each processor installed on the CPU socket has an integrated memory controller (IMC), which supports up to three DDR3 channels and groups DIMMs on the server boards into autonomous memory.

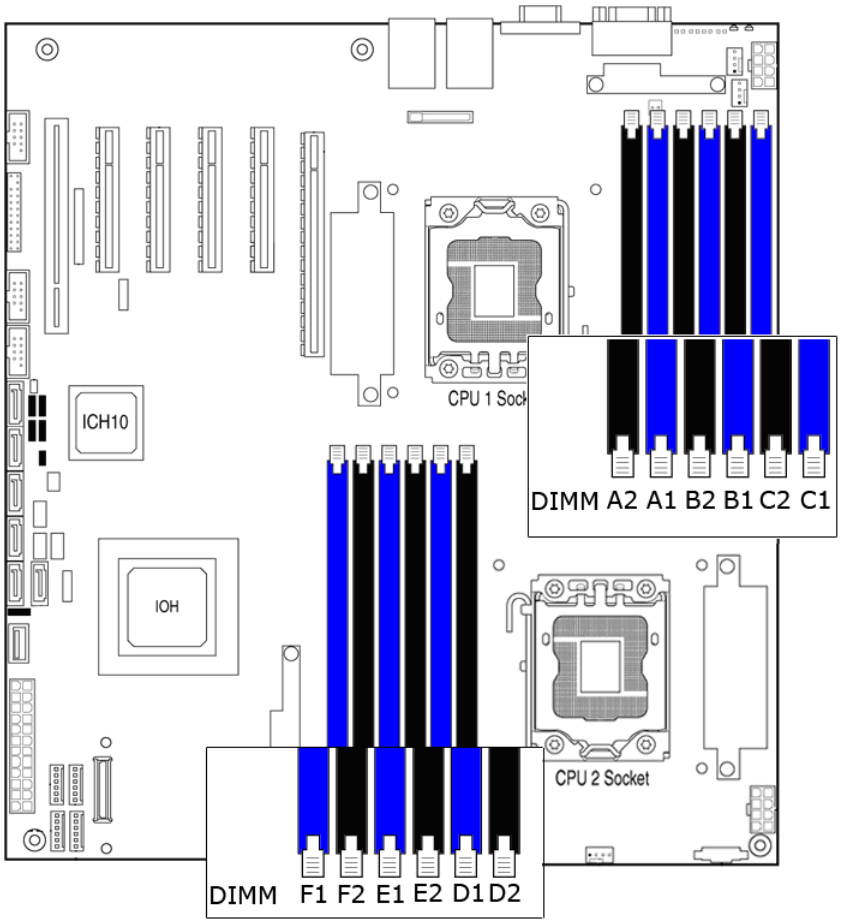
3.3.1 Memory Subsystem Nomenclature

The nomenclature for DIMM sockets implemented in the Intel® Server Boards S5520HC, S5500HCV and S5520HCT is represented in the following figures.

- DIMMs are organized into physical slots on DDR3 memory channels that belong to processor sockets.
- The memory channels for CPU 1 socket are identified as Channels A, B, and C. The memory channels for CPU 2 socket are identified as Channels D, E, and F.
- The DIMM identifiers on the silkscreen on the board provide information about which channel/CPU Socket they belong to. For example, DIMM_A1 is the first slot on Channel A of CPU 1 socket. DIMM_D1 is the first slot on Channel D of CPU 2 Socket.
- Processor sockets are self-contained and autonomous. However, all configurations in the BIOS setup, such as RAS, Error Management, and so forth, are applied commonly across sockets.

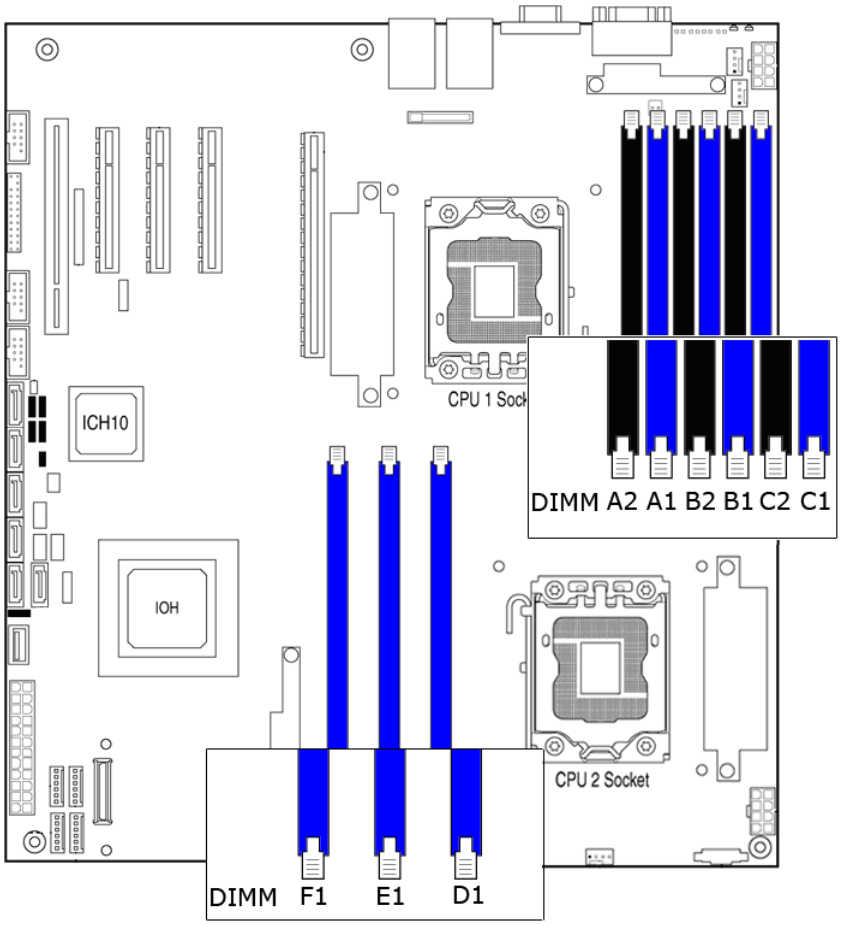
The Intel® Server Board S5520HC supports six DDR3 memory channels (three channels per processor) with two DIMM slots per channel, thus supporting up to twelve DIMMs in two-processor configuration. See Figure 16 for the Intel® Server Board S5520HC DIMM slots arrangement.

The Intel® Server Board S5500HCV supports six DDR3 memory channels (three channels per processor) with two DIMM slots per channel at Channels A, B, and C, and one DIMM slot per channel at Channels D, E, and F, thereby supporting up to nine DIMMs in a two-processor configuration. See Figure 17 for the Intel® Server Board S5500HCV DIMM slots arrangement.



Server Board	CPU Socket	DIMM Identifier	Channel/Slot
Intel® Server Board S5520HC	CPU 1	A1 (Blue)	Channel A, Slot 0
		A2 (Black)	Channel A, Slot 1
		B1 (Blue)	Channel B, Slot 0
		B2 (Black)	Channel B, Slot 1
		C1 (Blue)	Channel C, Slot 0
		C2 (Black)	Channel C, Slot 1
	CPU 2	D1 (Blue)	Channel D, Slot 0
		D2 (Black)	Channel D, Slot 1
		E1 (Blue)	Channel E, Slot 0
		E2 (Black)	Channel E, Slot 1
		F1 (Blue)	Channel F, Slot 0
		F2 (Black)	Channel F, Slot 1

Figure 16. Intel® Server Board S5520HC DIMM Slots Arrangement



Server Board	CPU Socket	DIMM Identifier	Channel/Slot
Intel® Server Board S5500HCV	CPU 1	A1 (Blue)	Channel A, Slot 0
		A2 (Black)	Channel A, Slot 1
		B1 (Blue)	Channel B, Slot 0
		B2 (Black)	Channel B, Slot 1
		C1 (Blue)	Channel C, Slot 0
		C2 (Black)	Channel C, Slot 1
	CPU 2	D1 (Blue)	Channel D, Slot 0
		E1 (Blue)	Channel E, Slot 0
		F1 (Blue)	Channel F, Slot 0

Figure 17. Intel® Server Board S5500HCV DIMM Slots Arrangement

3.3.2 Supported Memory

- Both Intel® Server Board S5520HC and Intel® Server Board S5500HCV support 1.5-V DDR3 DIMMs.
  - Intel® Server Board S5520HC supports up to 12 DIMMs with a maximum of 192GB memory capacity.
  - Intel® Server Board S5500HCV supports up to 9 DIMMs with a maximum of 144GB memory capacity.
- Both Intel® Server Board S5520HC and Intel® Server Board S5500HCV support Registered DDR3 DIMMs (RDIMMs), and ECC Unbuffered DDR3 DIMMs (UDIMMs).

- Mixing of RDIMMs and UDIMMs is not supported.
- Mixing memory type, size, speed and/or rank on this platform has not been validated and is not supported
- Mixing memory vendors is not supported on this platform by Intel
- Non-ECC memory is not supported and has not been validated in a server environment

- Both Intel® Server Board S5520HC and Intel® Server Board S5500HCV support the following DIMM and DRAM technologies:
  - RDIMMs:
    - Single-, Dual-, and Quad-Rank
    - x 4 or x8 DRAM with 1 Gb and 2 Gb technology, no support for 2 Gb DRAM based 2 GB or 4 GB RDIMMs
    - DDR3 1333 (Single- and Dual-Rank only), DDR3 1066, and DDR3 800
  - UDIMMs:
    - Single- and Dual-Rank
    - x8 DRAM with 1 Gb or 2 Gb technology
    - DDR3 1333, DDR3 1066, and DDR3 800

3.3.3 Processor Cores, QPI Links and DDR3 Channels Frequency Configuration

The Intel® Xeon® 5500 series processor connects to other Intel® Xeon® 5500 series processors and Intel® 5500/5520 IOH through the Intel® QPI link interface. The frequencies of the processor cores and the QPI links of Intel® Xeon® 5500 series processor are independent from each other. There are no gear-ratio requirements for the Intel® Xeon® Processor 5500 Series.

Intel® 5500/5520 IOH supports 4.8 GT/s, 5.86 GT/s, and 6.4 GT/s frequencies for the QPI links. During QPI initialization, the BIOS configures both endpoints of each QPI link to the same supportable speeds for the correct operation.

During memory discovery, the BIOS arrives at a fastest common frequency that matches the requirements of all components of the memory system and then configures the DDR3 DIMMs for the fastest common frequency.

In addition, rules on the following tables (Tables 3 and 4) also decide the global common memory system frequency.

Table 3. Memory Running Frequency vs. Processor SKU

		DIMM Type			
		DDR3 800	DDR3 1066	DDR3 1333	
Processor Integrated Memory Controller (IMC) Max. Frequency (Hz)	800	800	800	800	Memory Running Frequency (Hz) = Fastest Common Frequency of Processor IMC and Memory
	1066	800	1066	1066	
	1333	800	1066	1333	

Table 4. Memory Running Frequency vs. Memory Population

DIMM Type	DIMM Populated Per Channel	Memory Running Frequency (Y/N)			Command/Address Rate	Ranks Per DIMM SR: Single-Rank DR: Dual-Rank QR: Quad-Rank	Description
		800MHz	1066MHz	1333MHz			
RDIMM	1	Y	Y	Y	1N	SR or DR	All RDIMMs run at the fastes common frequency of processor IMCs and installed memory: 800MHz, 1066MHz or 133MHz
RDIMM	1	Y		N	1N	QR only	All RDIMMs run at 800MHz o 1066MHz when Quad-Rank RDIMM is installed in any channel.
RDIMM	2	Y	Y	N	1N	SR or DR	All RDIMMs run at 800MHz o 1066MHz when two RDIMMs (Single-Rank or Dual-Rank) are installed in the same channel.
RDIMM	2	Y	N	N	1N	QR only	All RDIMMs run at 800MHz when two RDIMMs (either or both are Quad-Rank RDIMM are installed in the same channel.
UDIMM w/ or w/o ECC	1	Y	Y	Y	1N	SR or DR	All UDIMMs run at the fastes common frequency of processor IMCs and installed memory: 800MHz, 1066MHz or 1333MHz.
UDIMM w/ or w/o ECC	2	Y	Y	N	2N	SR or DR	All UDIMMs run at 800MHz o 1066MHz when two UDIMMs (Single- or Dual-Rank) are installed in the same channe

1N: One clock cycle for the DRAM commands arrive at the DIMMs to execute.
2N: Two clock cycles for the DRAM commands arrive at the DIMMs to execute.

3.3.4 Publishing System Memory

- The BIOS displays the "***Total Memory***" of the system during POST if the "Quiet Boot" 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 also provides the total memory of the system in the BIOS setup (Main page and Advanced | Memory Configuration Page). This total is the same as the amount described by the previous bullet.
- The BIOS displays the "***Effective Memory***" of the system in the BIOS Setup (Advanced | Memory Configuration Page). The term Effective Memory refers to the total size of all active DDR3 DIMMs (not disabled) and not being used as redundant units in Mirrored Channel Mode.
- If Quiet 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.

3.3.4.1 Memory Reservation for Memory-mapped Functions

A region of size of 40 MB of memory below 4 GB is always reserved for mapping chipset, processor, and BIOS (flash) spaces as memory-mapped I/O regions. This region appears as a loss of memory to the operating system.

This (and other) reserved regions are reclaimed by the operating system if PAE is enabled in the operating system.

In addition to this memory reservation, the BIOS creates another reserved region for memory-mapped PCI Express* functions, including a standard 64 MB or 256 MB of standard PCI Express* MMIO configuration space. This is based on the setup selection, "Maximize Memory below 4GB".

If this is set to "Enabled", the BIOS maximizes usage of memory below 4 GB, for an operating system without PAE capability, by limiting PCI Express* Extended Configuration Space to 64 buses, rather than the standard 256 buses.

3.3.4.2 High-Memory Reclaim

When 4 GB or more of physical memory is installed (physical memory is the memory installed as DDR3 DIMMs), the reserved memory is lost. However, the Intel® 5500/5520 I/O Hub provides a feature called *high-memory reclaim*, which allows the BIOS and the operating system to remap the lost physical memory into system memory above 4 GB (the system memory is the memory the processor can see).

The BIOS always enables high-memory reclaim if it discovers installed physical memory equal to or greater than 4 GB. For the operating system, you can recover the reclaimed memory only if the PAE feature in the processor is supported and enabled. Most operating systems support this feature. For details, see your operating system's relevant manuals.

3.3.5 Memory Interleaving

The Intel® Xeon® Processor 5500 Series supports the following memory interleaving mode:

- Bank Interleaving – Interleave cache-line data between participant ranks.
- Channel Interleaving – Interleave between channel when not in Mirrored Channel Mode.
- Socket Interleaving – Interleaved memory can spread between both CPU sockets when NUMA mode is disabled, given both CPU sockets are populated and DDR3 DIMMs are installed in slots for both sockets.

3.3.6 Memory Test

3.3.6.1 Integrated Memory BIST Engine

The Intel® Xeon® Processor 5500 series incorporate an integrated Memory Built-in Self Test (BIST) engine enabled to provide extensive coverage of memory errors at both the memory cells and the data paths emanating from the DDR3 DIMMs.

The BIOS also uses the Memory BIST to initialize memory at the end of the memory discovery process.

3.3.7 Memory Scrub Engine

The Intel® Xeon® Processor 5500 Series incorporates a memory scrub engine, which performs periodic checks on the memory cells, and identifies and corrects single-bit errors. Two types of scrubbing operations are supported:

- ***Demand scrubbing*** – Executes when an error is encountered during normal read/write of data.
- ***Patrol scrubbing*** – Proactively walks through populated memory space seeking soft errors.

The BIOS enables both demand scrubbing and patrol scrubbing by default.

Demand scrubbing is not possible when memory mirroring is enabled. Therefore, if the memory is configured for mirroring, the BIOS disables it automatically.

3.3.8 Memory RAS

3.3.8.1 RAS Features

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT support the following memory channel modes:

- Independent Channel Mode
- Mirrored Channel Mode – providing Channel RAS feature

These channel modes are used in conjunction with the standard Memory Test (Built-in Self-Test (BIST) and Memory Scrub engines to provide full RAS support.

Channel RAS feature are supported only if both CPU sockets are populated and support the right population. For more information, refer to Section 3.3.9.

3.3.8.2 Independent Channel Mode

In the Independent Channel mode, you can populate multiple channels on any channel in any order. The Independent Channel mode provides less RAS capability but better DIMM isolation in case of errors. Moreover, it allows the best interleave mode possible and thereby increases performance and thermal characteristics.

Adjacent slots on a DDR3 Channel from the Intel® Xeon® Processor 5500 series do not need matching size and organization in independent channel mode. However, the speed of the channel is configured to the maximum common speed of the DIMMs.

The Single Channel mode is established using the Independent Channel mode by populating the DIMM slots from Channel A.

3.3.8.3 Mirrored Channel Mode

The Mirrored Channel mode is a RAS feature in which two identical images of memory channel data are maintained, providing maximum redundancy. On the Intel® Xeon® Processor 5500 series based Intel® server boards, the mirroring is achieved across channels. Active channels hold the primary image and the other channels hold the secondary image of the system memory. The integrated memory controller in the Intel® Xeon® Processor 5500 series alternates between both channels for read transactions. Write transactions are issued to both channels under normal circumstances. The mirrored image is a redundant copy of the primary image; therefore, the system can continue to operate despite the presence of sporadic uncorrectable errors, resulting in 100% data recovery.

In Mirrored Channel mode, channel A (or D) and channel B (or E) function as the mirrors, while Channel C (or F) is unused. The effective system memory is reduced by at least one-half. For example, if the system is operating in the Mirrored Channel mode and the total size of the DDR3 DIMMs is 2 GB, then the effective memory size is 1 GB because half of the DDR3 DIMMs are the secondary images.

If Channel C (or F) is populated, the BIOS will disable the Mirrored Channel mode. This is because the BIOS always gives preference to the maximization of memory capacity over memory RAS because RAS is an enhanced feature.

The BIOS provides a setup option to enable mirroring if the current DIMM population is valid for the Mirrored Channel mode of operation. When memory mirroring is enabled, the BIOS attempts to configure the memory system accordingly. If the BIOS finds the DIMM population is not suitable for mirroring, it falls back to the default Independent Channel mode with maximum interleaved memory.

3.3.9 Memory Population and Upgrade Rules

Populating and upgrading the system memory requires careful positioning of the DDR3 DIMMs based on the following factors:

- Current RAS mode of operation
- Existing DDR3 DIMM population
- DDR3 DIMM characteristics

- Optimization techniques used by the Intel® Xeon® Processor 5500 Series to maximize memory bandwidth

In the Independent Channel mode, all the DDR3 channels operate independently. Also, you can use the Independent Channel mode to support single DIMM configuration in Channel A and in the Single Channel mode.

You must observe and apply the following general rules when selecting and configuring memory to obtain the best performance from the system:

1. Mixing RDIMMs and UDIMMs is not supported.
2. You must populate CPU1 socket first in order to enable and operate CPU2 socket.
3. When CPU2 socket is empty, DIMMs populated in slots D1 through F2 are unusable.
4. If both CPU sockets are populated, but Channels A through C are empty, the platform can still function with remote memory in Channels D through F. However, platform performance suffers latency due to remote memory.
5. Must always start populating DDR3 DIMMs in the first slot on each memory channel (Memory slot A1, B1, C1, D1, E1, or F1). For example, if memory slot A1 is empty, slot A2 is not available.
6. Must always populate the Quad-Rank DIMM starting with the first slot (Memory slot A1, B1, C1, D1, E1, or F1) on each memory channel. For example, when installing one Quad-Rank RDIMM with one Single- or Dual-Rank RDIMM in memory channel A, you must populate the Quad-Rank RDIMM in slot A1.
7. If an installed DDR3 DIMM has faulty or incompatible SPD data, it is ignored during memory initialization and is (essentially) disabled by the BIOS. If a DDR3 DIMM has no or missing SPD information, the slot in which it is placed is treated as empty by the BIOS.
8. The memory operational mode is configurable at the channel level. The following two modes are supported: Independent Channel Mode and Mirrored Channel Mode.
9. The BIOS selects the mode that enables all the installed memory by default. Since the Independent Channel Mode enables all the channels simultaneously, this mode becomes the default mode of operation.
10. When only CPU1 socket is populated, Mirrored Channel mode is selected only if the DIMMs are populated to conform to that channel RAS mode. If it fails to comply with the population rule, then the BIOS configures the CPU1 socket to default to the Independent Channel mode.
11. If both CPU sockets are populated and the installed DIMMs are associated with both CPU sockets, then Mirrored Channel Mode can only be selected if **both** the CPU sockets are populated to conform to that mode. If either or both sockets fail to comply with the population rule, the BIOS configures both the CPU sockets to default to the Independent Channel mode.
12. DIMM parameters matching requirements for Mirrored Channel Mode is local to the CPU socket. For example, while CPU1 memory channels A, B, and C have one match of timing, technology and size, CPU 2 memory channels D, E, and F can have a different match of the parameters, channel RAS still functions.
13. The Minimal memory population possible is DIMM_A1. In this configuration, the system operates in the Independent Channel Mode. Mirrored Channel Mode is not possible.

14. The minimal population upgrade recommended for enabling CPU 2 socket are DIMM_A1 and DIMM_D1. This configuration supports only the Independent Channel mode.
15. In the Mirrored Channel mode, memory population on Channels A and B should be identical, including across adjacent slots on the channels, memory population on Channels D and E should be identical, including across adjacent slots on the channels. The DIMMs on successive slots are not required to be identical and can have different sizes and/or timings, but the overall channel timing reduces according to the slowest DIMM. If Channels A and B are not identical, or Channels D and E are not identical, the BIOS selects default Independent Channel Mode.
16. If Channel C or F is not empty, the BIOS disables the Mirrored Channel Mode.
17. When only CPU1 socket is populated, minimal population upgrade for Mirrored Channel Mode are DIMM_A1 and DIMM_B1. DIMM_A1 and DIMM_B1 must be identical, otherwise, they will revert to Independent Channel Mode.
18. When both CPU sockets are populated, minimal population upgrade for the Mirrored Channel Mode are DIMM_A1, DIMM_B1, DIMM_D1 and DIMM_E1. DIMM_A1 and DIMM_B1 as a pair must be identical, and so must DIMM_D1 and DIMM_E1 as a pair. The DIMMs on different CPU sockets need not be identical in size and/or sizing, although overall channel timing reduces according to the slowest DIMM.

3.3.10 Supported Memory Configuration

3.3.10.1 Supported Memory Configurations

The following sections describe the memory configurations supported and validated on the Intel® Server Boards S5520HC, S5500HCV and S5520HCT.

3.3.10.1.1 Levels of support

The following categories of memory configurations are supported:

- **Supported** – These configurations were verified by Intel to work but only limited validation was performed. Not all possible DDR3 DIMM configurations were validated due to the large number of possible configuration combinations. Supported configurations are highlighted in light gray in Tables 5 and 6.
- **Validated** – These configurations have received broad validation by Intel. Intel can provide customers with information on specific configurations that were validated. Validated configurations are highlighted in dark gray in Tables 5 and 6.
- All populated DIMMs are identical.

The following is a description of the columns in Tables 5 and 6:

- X – Indicates the DIMM is populated.
- M – Indicates whether the configuration supports the Mirrored Channel mode of operation. It is one of the following: **Y** indicating Yes; **N** indicating No.
- N – Identifies the total number of DIMMs that constitute the given configuration.

Table 5. Supported DIMM Population under the Dual Processors Configuration

#	N	CPU1 Socket = Populated						CPU2 Socket = Populated						M
		A1	A2	B1	B2	C1	C2	D1	D2	E1	E2	F1	F2	
1	1	X												N
2	2	X	X											N
3	2	X		X										N
4	2	X						X						N
5	3	X		X		X								N
6	3	X	X	X										N
7	3	X		X				X						N
8	4	X	X	X		X								N
9	4	X		X				X		X				Y
10	6	X	X	X	X			X		X				Y
11	6	X		X		X		X		X		X		N
12	7	X	X	X	X			X	X	X				N
13	8	X	X	X	X			X	X	X	X			Y
14	8	X	X	X		X		X	X	X		X		N
15	9	X	X	X	X	X	X	X		X		X		N
16	12	X	X	X	X	X	X	X	X	X	X	X	X	N

Table 6. Supported DIMM Population under the Single Processor Configuration

#	N	CPU1 Socket = Populated						CPU2 Socket = Empty						M
		A1	A2	B1	B2	C1	C2	D1	D2	E1	E2	F1	F2	
1	1	X												N
2	2	X	X											N
3	2	X		X										Y
4	3	X		X		X								N
5	4	X	X	X		X								N
6	4	X	X	X	X									Y
7	6	X	X	X	X	X	X							N

Note: The generic principles and guidelines described in the above sections also apply to the above two tables.

3.3.11 Memory Error Handling

The BIOS classifies memory errors into the following categories:

- **Correctable ECC errors**: This correction could be the result of an ECC correction, a successfully retried memory cycle, or both.
- **Unrecoverable/Fatal ECC Errors**: The ECC engine detects these errors but cannot correct them.
- **Address Parity Errors**: An Address Parity Error is logged as such in the SEL, but in all other ways, is treated the same as an Uncorrectable ECC Error.

3.4 ICH10R

The ICH10R provides extensive I/O support. Functions and capabilities include:

- PCI Express* Base Specification, Revision 1.1, support
- PCI Local Bus Specification, Revision 2.3, support for 33-MHz PCI operations (supports up to four REQ#/GNT# pairs)
- ACPI Power Management Logic Support, Revision 3.0a
- Enhanced DMA controller, interrupt controller, and timer functions
- Integrated Serial ATA host controllers with independent DMA operation on up to six ports and AHCI support
- USB host interface with support for up to 12 USB ports; six UHCI host controllers; and two EHCI high-speed USB 2.0 host controllers
- Integrated 10/100/1000 Gigabit Ethernet MAC with System Defense
- System Management Bus (SMBus) Specification, Version 2.0, with additional support for I^2C devices
- Low-Pin Count (LPC) interface support
- Firmware Hub (FWH) interface support
- Serial Peripheral Interface (SPI) support

3.4.1 Serial ATA Support

The ICH10R has an integrated Serial ATA (SATA) controller that supports independent DMA operation on six ports and supports data transfer rates of up to 3.0 Gb/s. The six SATA ports on the server boards are numbered SATA-0 through SATA-5. You can enable/disable the SATA ports and/or configure them by accessing the BIOS Setup utility during POST.

3.4.1.1 Intel® Embedded Server RAID Technology II Support

The Intel® Embedded Server RAID Technology II (Intel® ESRTII) feature provides RAID modes 0, 1, and 10. If RAID 5 is needed with Intel® ESRTII, you must install the optional Intel® RAID Activation Key AXXRAKSW5 accessory. You must place this activation key on the SATA Software RAID 5 connector located on the Intel® Server Boards S5520HC, S5500HCV and S5520HCT. For installation instructions, see the documentation accompanying the server boards and the activation key.

When Intel® Embedded Server RAID Technology II of the SATA controller is enabled, enclosure management is provided through the SATA_SGPIO connector on the server boards when a cable is attached between this connector and the backplane or I^2C interface.

See Figure 3, “Major Board Components” for the locations of Intel® RAID Activation Key connector and SATA SGPIO connector.

Intel® Embedded Server RAID Technology II functionality requires the following items:

- ICH10R I/O Controller Hub
- Software RAID option is selected on the BIOS menu for the SATA controller

- Intel® Embedded Server RAID Technology II Option ROM
- Intel® Embedded Server RAID Technology II drivers, most recent revision
- At least two SATA hard disk drives

3.4.1.1.1 Intel® Embedded Server RAID Technology II Option ROM

The Intel® Embedded Server RAID Technology II for SATA Option ROM provides a pre-operating system user interface for the Intel® Embedded Server RAID Technology II implementation and provides the ability to use an Intel® Embedded Server RAID Technology II volume as a boot disk and detect any faults in the Intel® Embedded Server RAID Technology II volume(s).

3.4.1.2 Onboard SATA Storage Mode Matrix

Table 7. Onboard SATA Storage Mode Matrix

SW RAID = Intel® Embedded Server RAID Technology II (ESRTII)

Storage Controller	Storage Mode*	Description	RAID Types and Levels Supported	Driver	RAID Management Software	RAID Software User's Guide	Compatible Backplane
Onboard SATA Controller (ICH10R)	Enhanced	6 SATA ports at Native mode	N/A	Chipset driver or operating system embedded Broad OS support	N/A	N/A	AXX6DRV3GR AXX4DRV3GR
	Compatibility	6 SATA ports: port 0, 1, 2, 3 at IDE Legacy mode, port 4, 5 at Native mode	N/A	Chipset driver or operating system embedded Broad OS support	N/A	N/A	
	AHCI	6 SATA ports using the Advanced Host Controller Interface	N/A	AHCI driver or OS embedded Broad OS support	N/A	N/A	
	SW RAID	6 SATA Ports	SW RAID 0/1/10 standard SW RAID 5 with optional AXXRAKSW5	ESRTII Driver Microsoft Windows* and selected Linux* Versions only	Intel® RAID Web Console 2	Intel® RAID Software User's Guide	

* Select in BIOS Setup: "SATA Mode" Option on Advanced | Mass Storage Controller Configuration Screen

3.4.2 USB 2.0 Support

The USB controller functionality integrated into the ICH10R provides the server boards with an interface for up to ten USB 2.0 ports. All ports are high-speed, full-speed, and low-speed capable.

- Four external connectors are located on the back edge of the server boards.
- One internal 2x5 header (J1D1) is provided, capable of supporting two optional USB 2.0 ports.
- One internal 2x5 header (J1D2) is provided for Intel® Server or Workstation chassis front panel USB ports, capable of supporting two optional USB 2.0 ports.
- One internal USB port type A connector (J1H2) is provided to support the installation of a USB device inside the server chassis.
- One internal low-profile 2x5 header (J2D2) is provided to support a low-profile USB Solid State Drive.

Note: Each USB port supports a maximum 500 mA current. Only supports up to eight USB ports to draw maximum current concurrently.

3.5 PCI Subsystem

The primary I/O buses for the Intel® Server Board S5520HC are PCI, PCI Express* Gen1, and PCI Express* Gen2 with six independent PCI bus segments.

The primary I/O buses for the Intel® Server Board S5500HCV are PCI, PCI Express* Gen1, and PCI Express* Gen2 with five independent PCI bus segments.

PCI Express* Gen1 and Gen2 are dual-simplex point-to-point serial differential low-voltage interconnects. A PCI Express* topology can contain a Host Bridge and several endpoints (I/O devices). The signaling bit rate is 2.5 Gb/s one direction per lane for Gen1 and 5.0 Gb/s one direction per lane for Gen2. Each port consists of a transmitter and receiver pair. A link between the ports of two devices is a collection of lanes (x1, x2, x4, x8, x16, and so forth). All lanes within a port must transmit data using the same frequency. The PCI buses comply with the *PCI Local Bus Specification*, Revision 2.3.

The following tables list the characteristics of the PCI bus segments. Details about each bus segment follow the tables.

Table 8. Intel® Server Board S5520HC PCI Bus Segment Characteristics

PCI Bus Segment	Voltage	Width	Speed	Type	PCI I/O Card Slots
PCI32 ICH10R	5 V	32 bit	33 MHz	PCI	PCI Slot 1
PE1, PE2, PE3, PE4 ICH10R PCI Express* Ports	3.3 V	x4	10 Gb/s	PCI Express* Gen1	x4 PCI Express* Gen1 throughput to Slot 2 (x8 mechanically) and Intel® SAS Entry RAID Module AXX4SASMOD slot (Default to Slot 2, and switch to SAS Module slot when Intel® SAS Entry RAID Module AXX4SASMOD is detected) This PCI Express* Gen1 slot is not available when the SAS module slot is in use and vice versa.
PE5 ICH10R PCI Express* Port	3.3 V	x1	2.5 Gb/s	PCI Express* Gen1	x1 PCI Express* Gen1 throughput to onboard Integrated BMC
PE1, PE2 5520 IOH PCI Express* Ports	3.3 V	x4	10 Gb/s	PCI Express* Gen1	x4 PCI Express* Gen1 throughput to onboard NIC (82575EB)
PE3, PE4 5520 IOH PCI Express* Ports	3.3 V	x8	40 Gb/S	PCI Express* Gen2	x8 PCI Express* Gen2 throughput to Slot 6 (x16 mechanically)
PE5, PE6 5520 IOH PCI Express* Ports	3.3 V	x8	40 Gb/S	PCI Express* Gen2	x8 PCI Express* Gen2 throughput to Slot 5 (x8 mechanically)
PE7, PE8 5520 IOH PCI Express* Ports	3.3 V	x8	40 Gb/S	PCI Express* Gen2	x8 PCI Express* Gen2 throughput to Slot 4 (x8 mechanically)
PE9, PE10 5520 IOH PCI Express* Ports	3.3 V	x8	40 Gb/S	PCI Express* Gen2	x8 PCI Express* Gen2 throughput to Slot 3 (x8 mechanically)

Table 9. Intel® Server Board S5500HCV PCI Bus Segment Characteristics

PCI Bus Segment	Voltage	Width	Speed	Type	PCI I/O Card Slots
PCI32 ICH10R	5 V	32 bit	33 MHz	PCI	PCI Slot 1
PE1, PE2, PE3, PE4 ICH10R PCI Express* Ports	3.3 V	x4	10 Gb/s	PCI Express* Gen1	x4 PCI Express* Gen1 throughput to Slot 2 and Intel® SAS Entry RAID Module AXX4SASMOD slot (x8 mechanically) (Default to Slot 2, and switch to SAS Module slot when Intel® SAS Entry RAID Module AXX4SASMOD is detected). This PCI Express* Gen1 slot is not available when the SAS module slot is in use and vice versa.
PE5 ICH10R PCI Express* Port	3.3 V	x1	2.5 Gb/s	PCI Express* Gen1	x1 PCI Express* Gen1 throughput to onboard Integrated BMC
PE1, PE2 5500 IOH PCI Express* Ports	3.3 V	x4	10 Gb/s	PCI Express* Gen1	x4 PCI Express* Gen2 throughput to onboard NIC (82575EB)
PE3 5500 IOH PCI Express* Port	3.3 V	x4	10 Gb/S	PCI Express* Gen2	x4 PCI Express* Gen1 throughput to Slot 6 (x16 mechanically)
PE7, PE8 5500 IOH PCI Express* Ports	3.3 V	x8	40 Gb/S	PCI Express* Gen2	x8 PCI Express* Gen2 throughput to Slot 4 (x8 mechanically)
PE9, PE10 5500 IOH PCI Express* Ports	3.3 V	x8	40 Gb/S	PCI Express* Gen2	x8 PCI Express* Gen2 throughput to Slot 3 (x8 mechanically)

3.5.1 PCI Express* Riser Slot (S5520HC – Slot 6)

One PCI Express* pin is designated as Riser Card Type pin with the definitions noted in the following table for Intel® Server Board S5520HC PCI Express* slot 6.

Table 10. Intel® Server Board S5520HC PCI Riser Slot (Slot 6)

PCI Express* Gen2 Slot 6 Setup[1]	IOH PEWIDTH [2] PCI Riser Strap	
	PCI Express* Pin	A50 [RVSD]
Type 1 Riser, One x8 PCI Express* Slot2	1	
Type 2 Riser, Two x4 PCI Express* Slot3	0	

1. Maximum power rating of Slot 6 for riser is 75 W, provided no card is in slots 3, 4, and 5.
2. The type 1 riser card must follow the standard PCI Express* Adapter pin-out and leave pin A50 as a No-Connect (NC).
3. The type 2 riser card must connect the PCI Express* pin A50 with a 4.7K ohm resistor to pull up to 3.3 V.

The following table provides the supported bus throughput for the given riser card used and the number of add-in cards installed.

Table 11. PCI Riser Support

PCI Express* Gen2 Slot 6 Riser Support	One Add-in card	Two Add-in cards
Type 1 Riser Card	x8	N/A
Type 2 Riser Card	x4	x4

There are no population rules for installing a single add-in card in the Type 2 riser card; you can install a single add-in card in either PCI Express* slot.

3.6 Intel® SAS Entry RAID Module AXX4SASMOD (Optional Accessory)

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT provide a Serial Attached SCSI (SAS) module slot (J2J1) for the installation of an optional Intel® SAS Entry RAID Module AXX4SASMOD. Once the optional Intel® SAS Entry RAID Module AXX4SASMOD is detected, the x4 PCI Express* links from the ICH10R to Slot 2 (x8 mechanically, x4 electrically) switches to the SAS module slot.

The Intel® SAS Entry RAID Module AXX4SASMOD includes a SAS1064e controller that supports x4 PCI Express* link widths and is a single-function PCI Express* end-point device. The SAS controller supports the SAS protocol as described in the Serial Attached SCSI Standard, version 1.0, and also supports SAS 1.1 features. A 32-bit external memory bus off the SAS1064e controller provides an interface for Flash ROM and NVSRAM (Non-volatile Static Random Access Memory) devices.

The Intel® SAS Entry RAID Module AXX4SASMOD provides four SAS connectors that support up to four hard drives with a non-expander backplane or up to eight hard drives with an expander backplane.

The Intel® SAS Entry RAID Module AXX4SASMOD also provides a SGPIO (Serial General Purpose Input/Output) connector and a SCSI Enclosure Services (SES) connector for backplane drive LED control.

***Warning*:** Either the SGPIO or the SES connector supports backplane drive LED control. Do not connect both SGPIO and SES connectors at the same time.

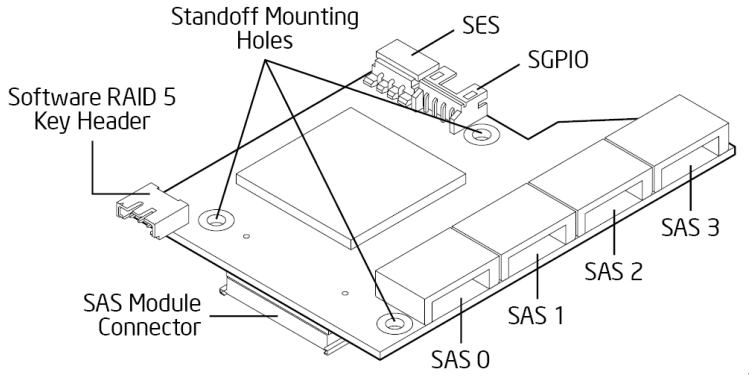


Figure 18. Intel® SAS Entry RAID Module AXX4SASMOD Component and Connector Layout

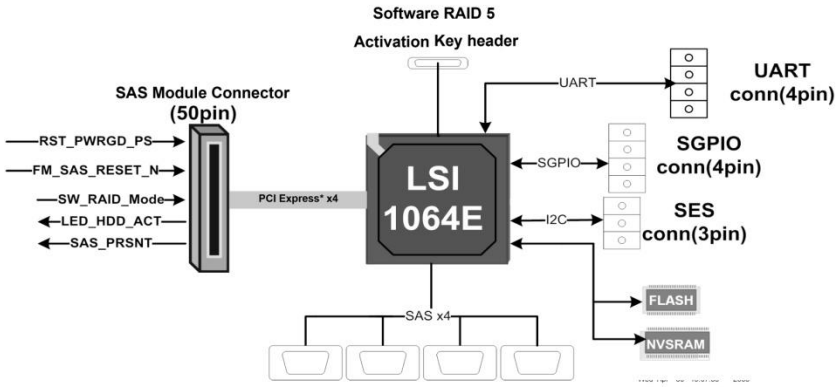


Figure 19. Intel® SAS Entry RAID Module AXX4SASMOD Functional Block Diagram

3.6.1 SAS RAID Support

The BIOS Setup Utility provides drive configuration options on the Advanced | Mass Storage Controller Configuration setup page for the Intel® SAS Entry RAID Module AXX4SASMOD, some of which affect the ability to configure RAID.

The “Intel® SAS Entry RAID Module” option is enabled by default once the Intel® SAS Entry RAID Module AXX4SASMOD is present. When enabled, you can set the “Configure Intel® SAS Entry RAID Module” to either “LSI* Integrated RAID” or “Intel® ESRTII” mode.

Table 12. Intel® SAS Entry RAID Module AXX4SASMOD Storage Mode

SW RAID = Intel® Embedded Server RAID Technology II (ESRTII)

IT/IR RAID = IT/IR RAID, Entry Hardware RAID

Storage Mode*	Description	RAID Types and Levels Supported	Driver	RAID Management Software	RAID Software User's Guide	Compatible Backplane
IT/IR RAID	4 SAS Ports Up to 10 SAS or SATA drives via expander backplanes	Native SAS pass through mode without RAID function. Entry Hardware RAID. RAID 1 (IM mode) RAID 10/10E (IME mode) RAID 0 (IS Mode)	SAS MPT driver (Fully open-source driver) Broad OS support.	Intel® RAID Web Console 2	IT/IR RAID Software User's Guide	AXX6DRV3GR AXX4DRV3GR AXX6DRV3GEXP AXX4DRV3GEXP
SW RAID	4 SAS Ports Up to 8 SAS or SATA drives via expander backplanes	SW RAID 0/1/10 standard SW RAID 5 with optional AXXRAKSW5	ESRTII Driver Microsoft Windows* and selected Linux* Versions only	Intel® RAID Web Console 2	Intel® RAID Software User's Guide	

*Select in BIOS Setup: "Configure Intel® SAS Entry RAID" Option on Advanced | Mass Storage Controller Configuration Screen

3.6.1.1 IT/IR RAID Mode

Supports entry hardware RAID 0, RAID 1, and RAID 1E and native SAS pass-through mode.

3.6.1.2 Intel® ESRTII Mode

The Intel® Embedded Server RAID Technology II (Intel® ESRTII) feature provides RAID modes 0, 1, and 10. If RAID 5 is needed with Intel® ESRTII, you must install the optional Intel® RAID Activation Key AXXRAKSW5 accessory. This activation key is placed on the SAS Software RAID 5 connector located on the Intel® SAS Entry RAID Module AXX4SASMOD. For installation instructions, see the documentation included with the SAS Module AXX4SASMOD and the activation key.

When Intel® Embedded Server RAID Technology II is enabled with the SAS Module AXX4SASMOD, enclosure management is provided through the SAS_SGPIO or SES connector on the SAS Module AXX4SASMOD when a cable is attached between this connector and the backplane or I^2C interface.

3.7 Baseboard Management Controller

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT have an integrated BMC controller based on ServerEngines* Pilot II. The BMC controller is provided by an embedded ARM9 controller and associated peripheral functionality that is required for IPMI-based server management.

The following is a summary of the BMC management hardware features used by the BMC:

- 250 MHz 32-bit ARM9 Processor
- Memory Management Unit (MMU)
- Two 10/100 Ethernet Controllers with NC-SI support
- 16-bit DDR2 667 MHz interface
- Dedicated RTC
- 12 10-bit ADCs
- Eight Fan Tachometers
- Four PWMs
- Battery-backed Chassis Intrusion I/O Register
- JTAG Master
- Six I^2C interfaces
- General-purpose I/O Ports (16 direct, 64 serial)

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

- Keyboard style/BT interface
- Two 16550-compatible serial ports
- Serial IRQ support
- 16 GPIO ports (shared with the BMC)
- LPC to SPI bridge for system BIOS support
- SMI and PME support

The BMC also contains an integrated KVMS subsystem and graphics controller with the following features:

- USB 2.0 for Keyboard, Mouse, and Storage devices
- USB 1.1 interface for legacy PS/2 to USB bridging.
- Hardware Video Compression for text and graphics
- Hardware encryption
- 2D Graphics Acceleration
- DDR2 graphics memory interface
- Up to 1600x1200 pixel resolution
- PCI Express* x1 support

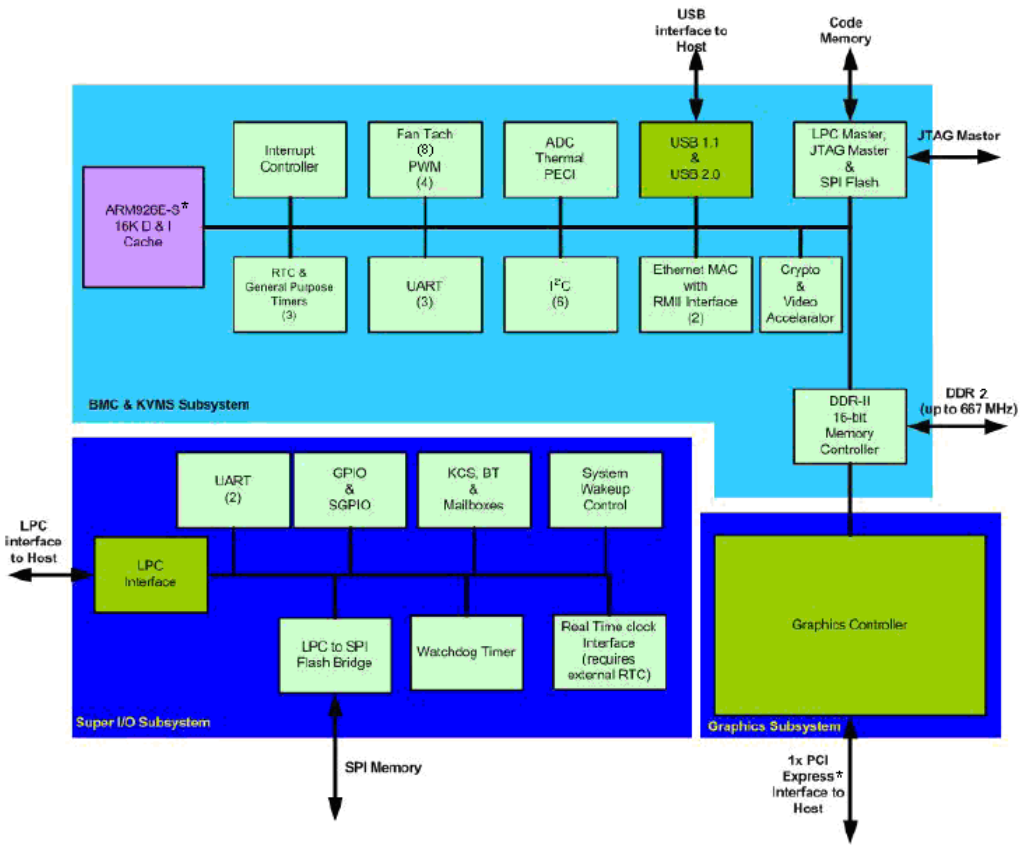


Figure 20. Integrated BMC Hardware

3.7.1 BMC Embedded LAN Channel

The BMC hardware includes two dedicated 10/100 network interfaces, which are given below:

Interface 1: This interface is available from either of the available NIC ports in system that can be shared with the host. Only one NIC may be enabled for management traffic at any time. The default active interface is onboard NIC1.

Interface 2: This interface is available from Intel® Remote Management Module 3 (Intel® RMM3), which is a dedicated management NIC and not shared with the host.

For these channels, you can enable support for IPMI-over-LAN and DHCP.

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

- IP Address: Static
- All users disabled

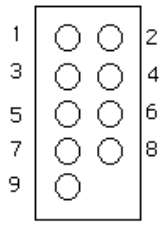
IPMI-enabled network interfaces may not be placed on the same subnet. This includes the Intel® RMM3's onboard network interface and either of the BMC's embedded network interfaces.

3.8 Serial Ports

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT provide two serial ports: an external DB9 serial port and an internal DH-10 serial header. The rear DB9 serial A port is a fully-functional serial port that can support any standard serial device.

Serial B is an optional port accessible through a 9-pin internal DH-10 header. You can use a standard DH-10 to DB9 cable to direct serial B to the rear of a chassis. The serial B interface follows the standard RS232 pin-out as defined in the following table.

Table 13. Serial B Header Pin-out

Pin	Signal Name	Serial Port B Header Pin-out
1	DCD	
2	DSR	
3	RX	
4	RTS	
5	TX	
6	CTS	
7	DTR	
8	RI	
9	GND	

3.9 Floppy Disk Controller

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT do not support a floppy disk controller interface. However, the system BIOS recognizes USB floppy devices.

3.10 Keyboard and Mouse Support

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT do not support PS/2* interface keyboards and mice. However, the system BIOS recognizes USB Specification-compliant keyboards and mice.

3.11 Video Support

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT integrated BMC include a 2D SVGA video controller and 8 MB video memory.

The 2D SVGA subsystem supports a variety of modes, up to 1024 x 768 resolution in 8/16/24/32 bpp. It also supports both CRT and LCD monitors with up to an 85-Hz vertical refresh rate.

Video is accessed using a standard 15-pin VGA connector found on the back edge of the server boards. You can disable the onboard video controller using the BIOS Setup Utility or when an add-in video card is detected. The system BIOS provides the option for Dual Monitor Video operation when an add-in video card is configured in the system.

3.11.1 Video Modes

The integrated video controller supports all standard IBM* VGA modes. The following table shows the 2D modes supported for both CRT and LCD.

Table 14. Video Modes

2D Mode	2D Video Mode Support				
	8 bpp	16 bpp	24 bpp	32 bpp	
640 x 480	Supported	Supported	Supported	Supported	
	60, 72, 75, 85	60, 72, 75, 85	60, 72, 75, 85	60, 72, 75, 85	Refresh Rate (Hz)
800 x 600	Supported	Supported	Supported	Supported	
	56, 60, 72, 75, 85	56, 60, 72, 75, 85	56, 60, 72, 75, 85	56, 60, 72, 75, 85	Refresh Rate (Hz)
1024 x 768	Supported	Supported	Supported	Supported	
	60, 70, 75, 85	60, 70, 75, 85	60, 70, 75, 85	60, 70, 75, 85	Refresh Rate (Hz)
1152 x 864	Supported	Supported	Supported	N/A	
	75	75	75	N/A	Refresh Rate (Hz)
1280 x 1024	Supported	Supported	Supported	N/A	
	60, 75, 85	60, 75, 85	60	NA	Refresh Rate (Hz)
1440 x 900	Supported	Supported	Supported	N/A	
	60	60	60	NA	Refresh Rate (Hz)
1600 x 1200	Supported	Supported	N/A	N/A	
	60. 65, 70, 75, 85	60. 65, 70	N/A	N/A	Refresh Rate (Hz)

3.11.2 Dual Video

The BIOS supports single- and dual-video modes. The dual-video mode is enabled by default.

- In single mode, the onboard video controller is disabled when an add-in video card is detected.
- In dual mode (enable "*Dual Monitor Video*" in the BIOS setup), the onboard video controller is enabled and is the primary video device. The add-in video card is allocated resources and considered the secondary video device.
- The BIOS Setup utility provides options on *Advanced* | *PCI Configuration Screen* to configure the feature as follows:

Onboard Video	Enabled (default)	
	Disabled	
Dual Monitor Video	Enabled	Shaded if onboard video is set to "Disabled"
	Disabled (Default)	

3.12 Network Interface Controller (NIC)

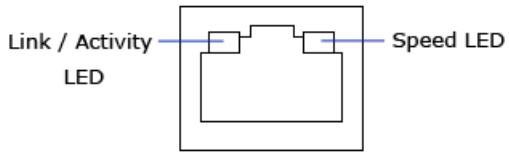
The Intel® Server Boards S5520HC, S5500HCV and S5520HCT provide dual onboard LAN ports with support for 10/100/1000 Mbps operation. The two LAN ports are based on the onboard Intel® 82575EB controller, which is a single, compact component with two, fully-integrated GbE Media Access Control (MAC) and Physical Layer (PHY) ports.

The Intel® 82575EB controller provides a standard IEEE 802.3 Ethernet interface for 1000BASE-T, 100BASE-TX, and 10BASE-T applications (802.3, 802.3u, and 802.3ab) and is capable of transmitting and receiving data at rates of 1000 Mbps, 100 Mbps, or 10 Mbps.

Each network interface controller (NIC) port provides two LEDs:

- Link/activity LED (at the left of the connector): Indicates network connection when on, and transmit/receive activity when blinking.
- The speed LED (at the right of the connector) indicates 1000-Mbps operation when amber; 100-Mbps operation when green; and 10-Mbps when off. The following table provides an overview of the LEDs.

Table 15. Onboard NIC Status LED



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

3.12.1 MAC Address Definition

Each Intel® Server Board S5520HC or S5500HCV has the following four MAC addresses assigned to it at the Intel factory.

- NIC 1 MAC address
- NIC 2 MAC address - is assigned the NIC 1 MAC address +1
- BMC LAN Channel MAC address – is assigned the NIC 1 MAC address +2
- Intel® Remote Management Module 3 (Intel® RMM3) MAC address – is assigned the NIC 1 MAC address +3

During the manufacturing process, each server board has a white MAC address sticker placed on the top of the NIC 1 port. The sticker displays the NIC 1 MAC address and Intel® RMM3 MAC in both bar code and alphanumeric formats.

3.13 *Trusted Platform Module (TPM) – Supported only on S5520HCT

3.13.1 Overview

Trusted Platform Module (TPM) 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 Intel® Server Board S5520HCT implements TPM as per TPM PC Client specifications revision 1.2 by the Trusted Computing Group (TCG).

A TPM device is affixed to the motherboard of the server 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 BIOS complete 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 TPM-enabled, 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).

3.13.2 TPM security BIOS

The BIOS TPM support conforms to the TPM PC Client Specific – Implementation Specification for Conventional BIOS, version 1.2, and to the TPM Interface specification, version 1.2. The BIOS adheres to the Microsoft Vista* BitLocker requirement. 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.

3.13.2.1 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).

3.13.2.2 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.

3.13.2.3 Security Screen

The Security screen provides fields 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 S5520HCT provides TPM settings through the security screen.

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

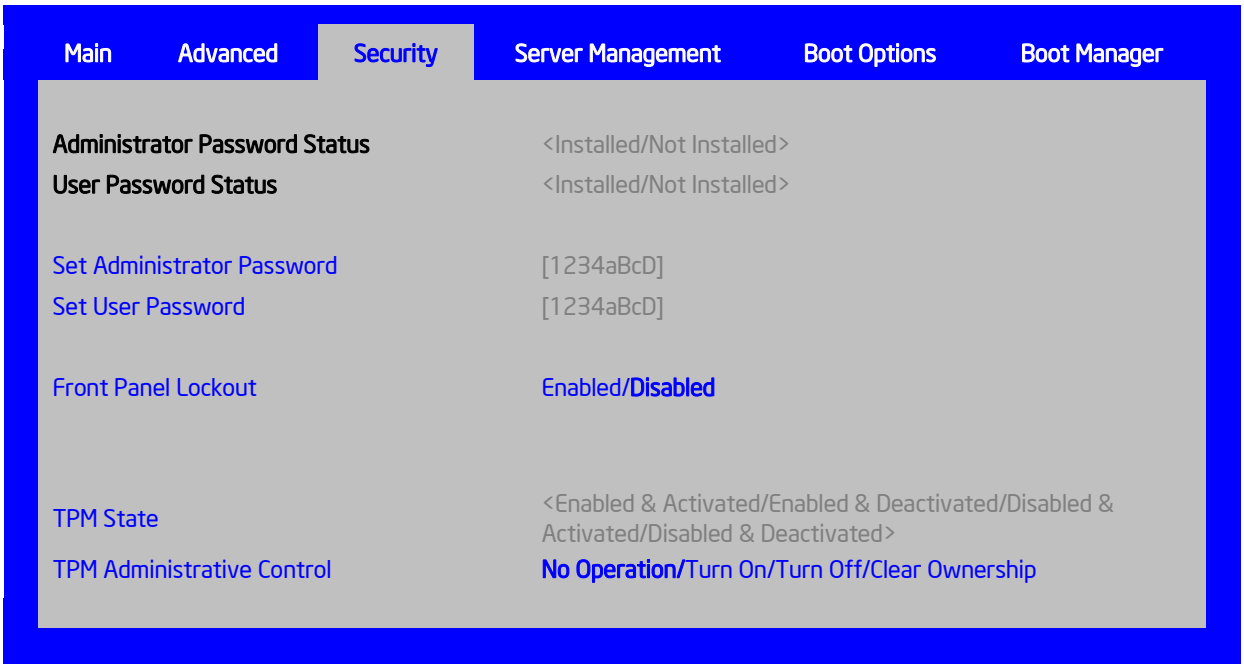


Figure 21. Setup Utility – TPM Configuration Screen

Table 16. TPM Setup 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.	

3.13.3 Intel® Trusted Execution Technology (Intel® TXT)

3.13.3.1 Overview

Intel® Trusted Execution Technology (Intel® TXT) for safer computing, formerly code named LaGrande Technology, is a versatile set of hardware extensions to Intel® processors and chipsets that enhance the platform with security capabilities such as measured launch and protected execution. Intel® TXT provides hardware-based mechanisms that help protect against software-based attacks and protects the confidentiality and integrity of data stored or created on the system. It does this by enabling an environment where applications can run within their own space, protected from all other software on the system. These capabilities provide the protection mechanisms, rooted in hardware, that are necessary to provide trust in the application's execution environment. In turn, this can help to protect vital data and processes from being compromised by malicious software running on the platform. Long available on client platforms, Intel is now enabling Intel TXT on selected server platforms as well.

3.13.3.2 Intel® TXT hardware overview

Implementation of a Trusted Execution Technology-enabled platform requires a number of hardware enhancements. Key hardware elements of this platform are:

Processor: Extensions to the IA-32 architecture allow for the creation of multiple execution environments, or partitions. This allows for the coexistence of a standard (legacy) partition and protected partition, where software can run in isolation in the protected partition, free from being observed or compromised by other software running on the platform. Access to hardware resources (such as memory) is hardened by enhancements in the processor and chipset hardware. Other processor enhancements include: (1) event handling, to reduce the vulnerability of data exposed through system events, (2) instructions to manage the protected execution environment, (3) and instructions to establish a more secure software stack.

Chipset: Extensions to the chipset deliver support for key elements of this new, more protected platform. They include: (1) the capability to enforce memory protection policy, (2) enhancements to protect data access from memory, (3) protected channels to graphics and input/output devices, (4) and interfaces to the Trusted Platform Module [Version 1.2].

Keyboard and Mouse: Enhancements to the keyboard and mouse enable communication between these input devices and applications running in a protected partition to take place without being observed or compromised by unauthorized software running on the platform.

Graphics: Enhancements to the graphic subsystem enable applications running within a protected partition to send display information to the graphics frame buffer without being observed or compromised by unauthorized software running on the platform.

The TPM v. 1.2 device: Also called the Fixed Token, is bound to the platform and connected to the PC's LPC bus. The TPM provides the hardware-based mechanism to store or 'seal' keys and other data to the platform. It also provides the hardware mechanism to report platform attestations.

3.13.3.3 Enabling Intel® TXT on Intel® Server Board

Intel® TXT can be supported by Intel® Server Board S5520HCT (PBA# E80888-553 or later version), following steps describe how to set up Intel® TXT feature:

System pre-requirements:

Processor: B1 or later stepping Intel® Xeon Processor 5600 Series
Server Board: Intel® Server Board S5520HCT; PBA version E80888-553 or later
Memory: At least 1 GB memory installed

Intel® TXT Setup:

1 – Enable TPM module:
Go to BIOS setup Menu page, **Security** Tab, set administrator password.

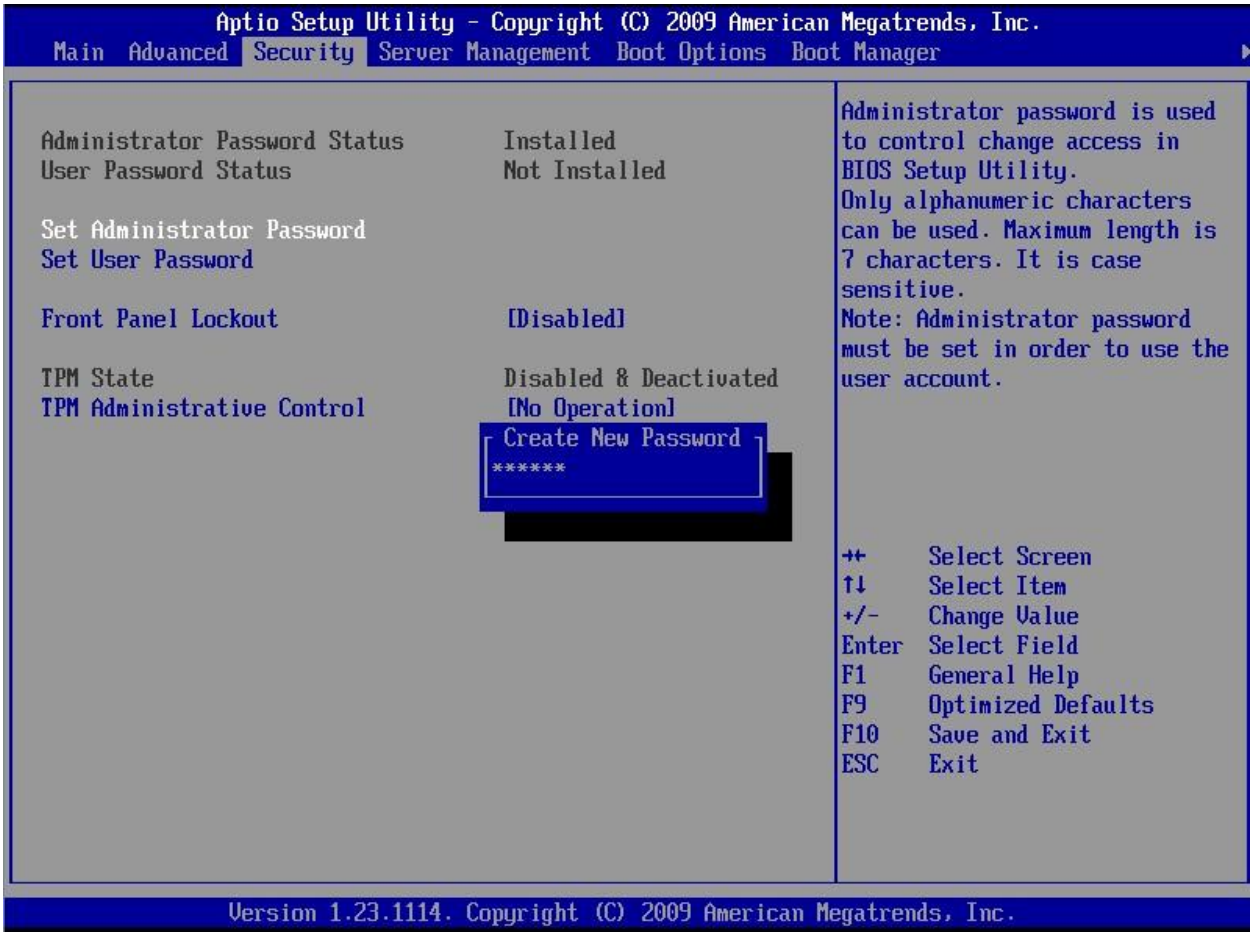


Figure 22. Setting Administrator password in BIOS

2. After administrator password is setup, press “F10” to save and exit BIOS setup.

3. System will automatically reboot, go to BIOS setup Menu page, **Security** Tab, set **TPM Administrative Control** as “**Turn ON**”, press “F10” to save and exit BIOS setup.

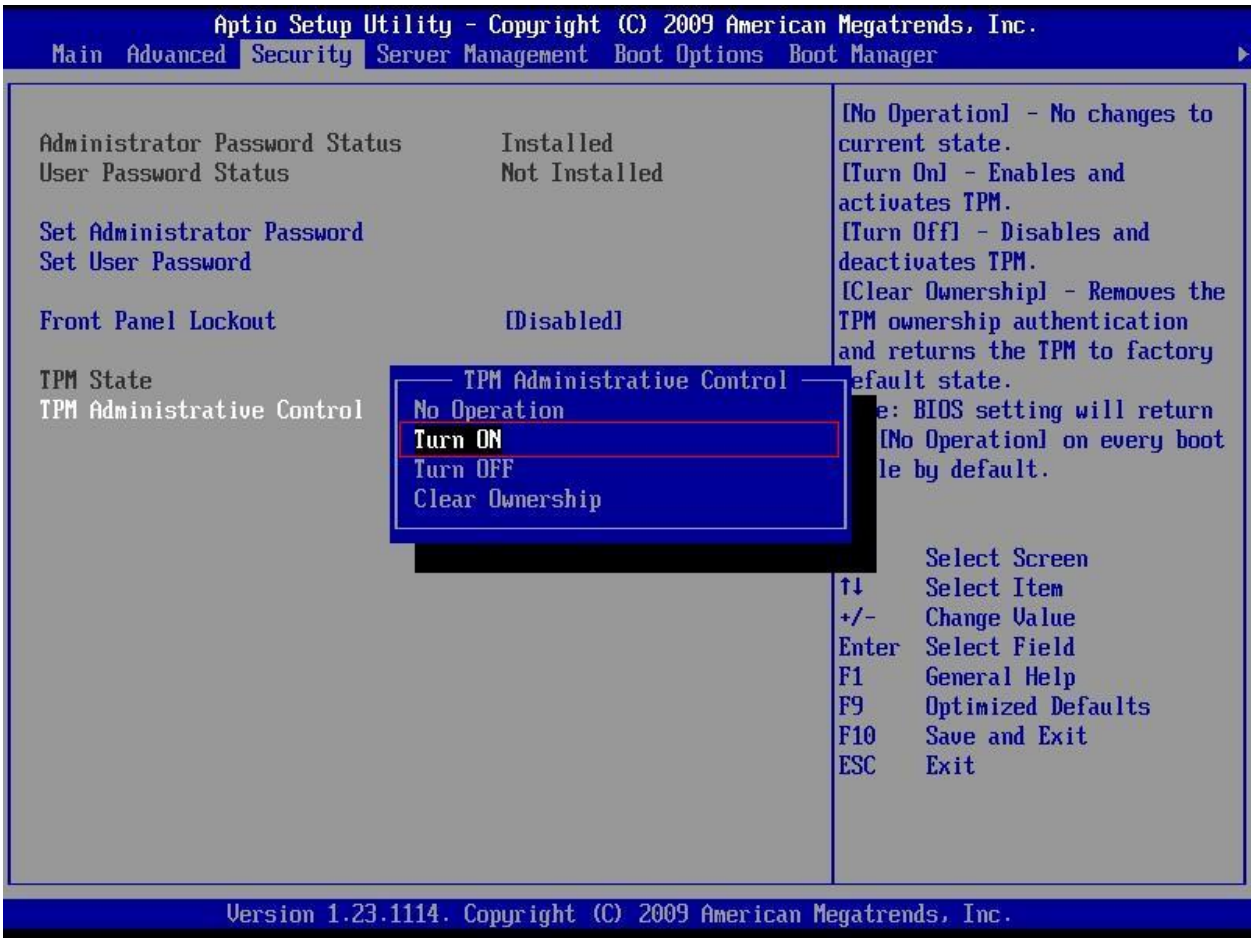


Figure 23. Activating TPM

4. Go to BIOS setup Menu, **Security** Tab, TPM State should be "**Enabled & Activated**".

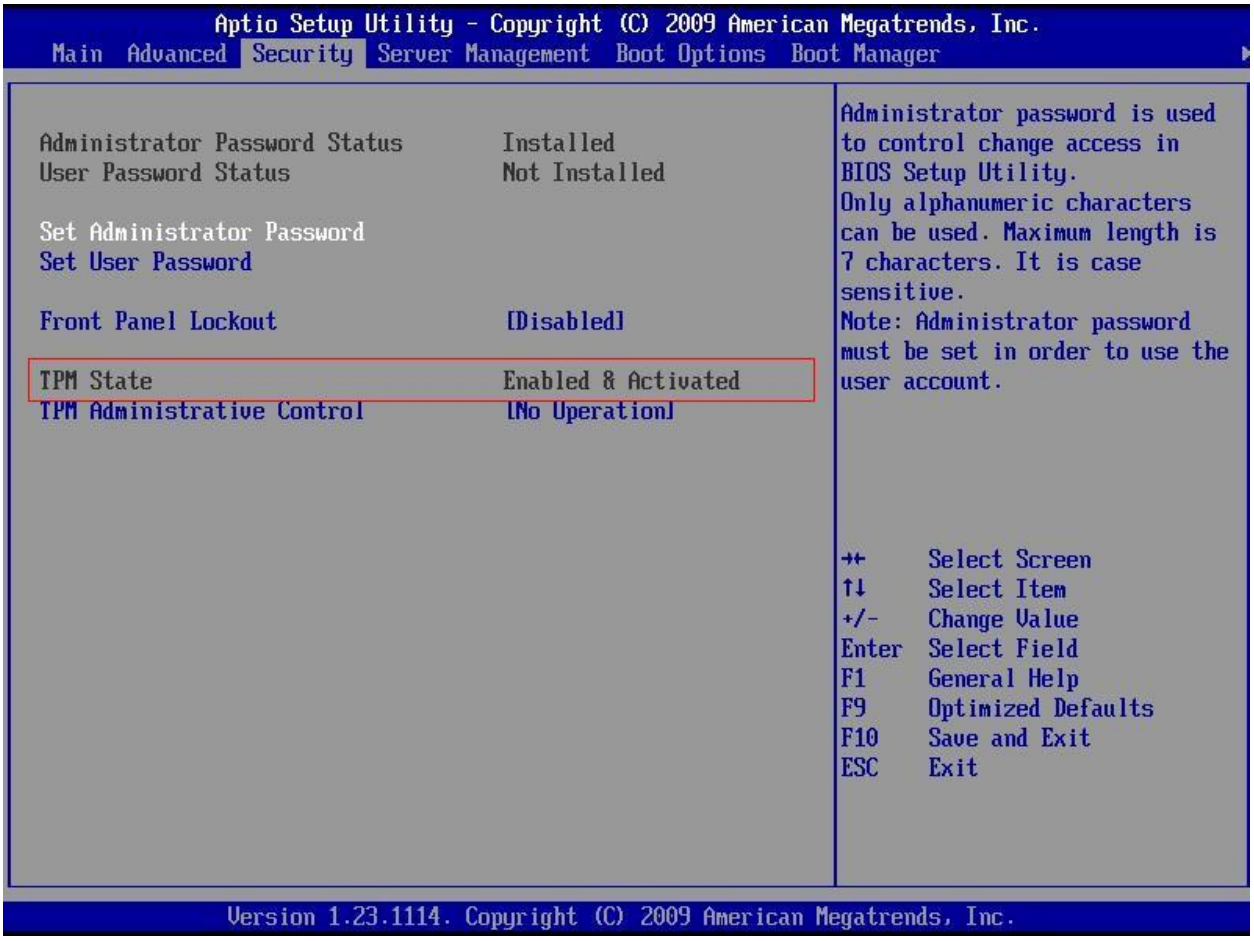


Figure 24. TPM activated

5. Go to BIOS Setup Menu, **Advanced** -> **Processor Configuration**, set **Intel® VT for directed I/O** and **Intel® TXT** option as "**Enabled**"

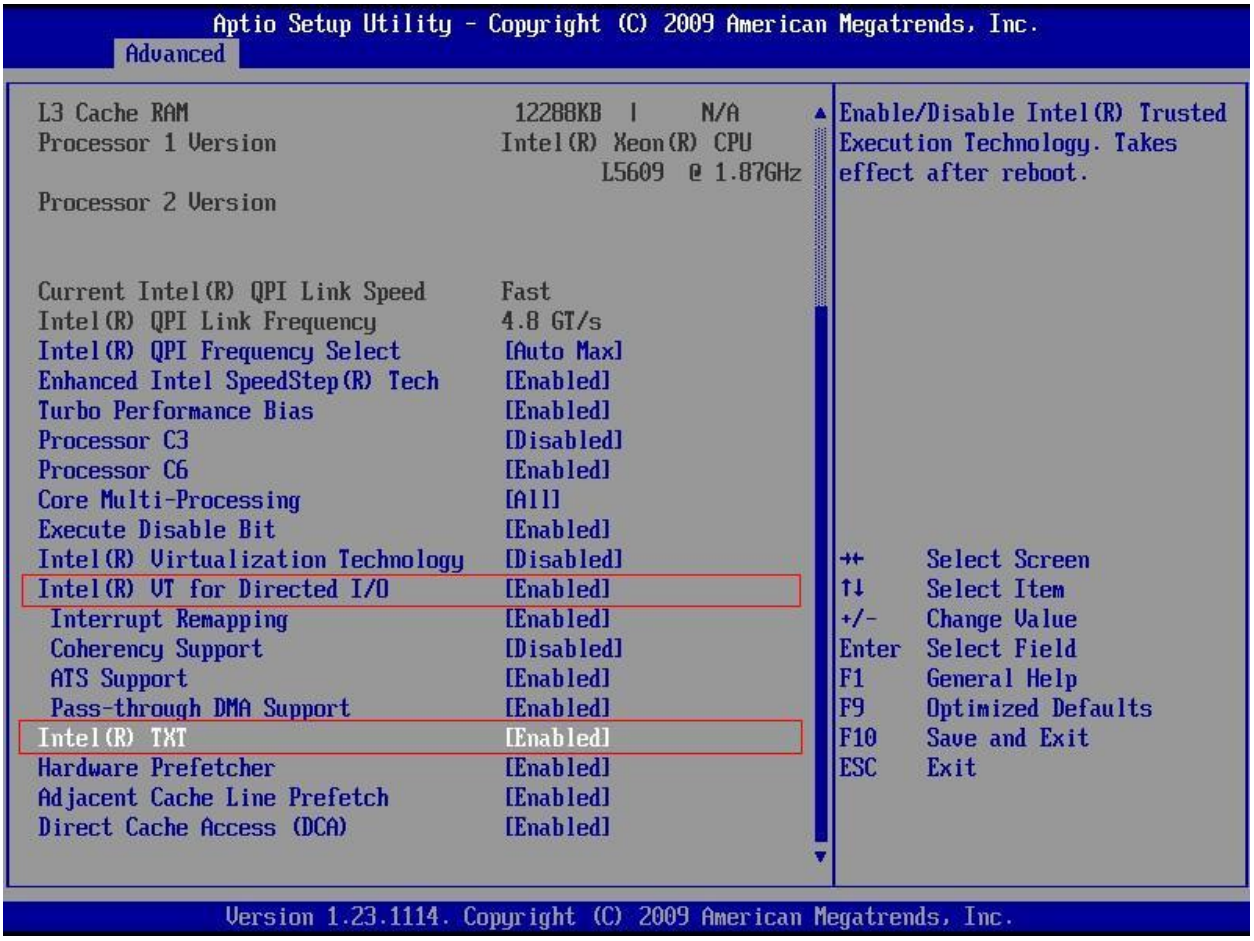


Figure 25. BIOS setting for TXT

6. Press “F10” to save and exit, now Intel® TXT is successfully enabled.

3.14 ACPI Support

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT support S0, S1, and S5 states. S1 is considered a sleep state.

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT can wake up from S1 state using the USB devices in addition to the sources described in the following paragraph.

The wake-up sources are enabled by the ACPI operating systems with cooperation from the drivers; the BIOS have no direct control over the wake-up sources when an ACPI operating system is loaded. The role of the BIOS is limited to describing the wake-up sources to the operating system.

The S5 state is equivalent to the operating system shutdown. No system context is saved when going into S5.

3.15 Intel® Virtualization Technology

Intel® Virtualization Technology is designed to support multiple software environments sharing the same hardware resources. Each software environment may consist of an operating system and applications. You can enable or disable the Intel® Virtualization Technology in the BIOS Setup. The default behavior is disabled.

Note: After changing the Intel® Virtualization Technology option (disable or enable) in the BIOS setup, users must perform an AC power cycle before the change takes effect.

3.15.1 Intel® Virtualization Technology for Directed IO (VT-d)

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT support DMA remapping from inbound PCI Express* memory Guest Physical Address (GPA) to Host Physical Address (HPA). PCI devices are directly assigned to a virtual machine leading to a robust and efficient virtualization.

You can enable or disable the Intel® Virtualization Technology for Directed I/O in the BIOS Setup. The default behavior is disabled.

Note: After changing the Intel® Virtualization Technology for Directed I/O options (disable or enable) in the BIOS setup, users must perform an AC power cycle before the changes can take effect.

4. Platform Management

The platform management subsystem is based on the Integrated BMC features of the ServerEngines* Pilot II. The onboard platform management subsystem consists of communication buses, sensors, and the system BIOS, and server management firmware. Figure 27 provides an illustration of the Server Management Bus (SMBUS) architecture as used on these server boards.

4.1 Feature Support

4.1.1 IPMI 2.0 Features

- Baseboard management controller (BMC).
- IPMI Watchdog timer.
- Messaging support, including command bridging and user/session support.
- Chassis device functionality, including power/reset control and BIOS boot flags support.
- Event receiver device: The BMC receives and processes events from other platform subsystems.
- Field replaceable unit (FRU) inventory device functionality: The BMC supports access to system FRU devices using IPMI FRU commands.
- System event log (SEL) device functionality: The BMC supports and provides access to a SEL.
- Sensor data record (SDR) repository device functionality: The BMC supports storage and access of system SDRs.
- Sensor device and sensor scanning/monitoring: The BMC provides IPMI management of sensors. It polls sensors to monitor and report system health.
- IPMI interfaces:
  - Host interfaces include system management software (SMS) with receive message queue support and server management mode (SMM).
  - IPMB interface.
  - LAN interface that supports the IPMI-over-LAN protocol (RMCP, RMCP+).
- Serial-over-LAN (SOL)
- ACPI state synchronization: The BMC tracks ACPI state changes provided by the BIOS.
- 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 v2.0*.

4.1.2 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 (dependant on platform support)
- Basic fan control using TControl version 2 SDRs
- Fan redundancy monitoring and support
- Power supply redundancy monitoring and support
- Hot swap fan support
- Acoustic management: Supports 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 Manger support

4.2 Optional Advanced Management Feature Support

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

Table 17 lists basic and advanced feature support. Individual features may vary by platform. For more information, refer to Appendix C.

Table 17. Basic and Advanced Management 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
SSH Support	X	X
Integrated KVM		X
Integrated Remote Media Redirection		X
Lightweight Directory Access Protocol (LDAP) for Linux		X
Intel® Intelligent Power Node Manager Support***	X	X
SMASH CLP	X	X
WS-Management		X

* Basic management features provided by integrated BMC
**Advanced management features available with optional Intel® Remote Management Module 3
***Intel® Intelligent Power Node Manager Support requires PMBus-compliant power supply

4.2.1 Enabling Advanced Management Features

BMC will enable advanced management features only when it detects the presence of the Intel® Remote Management Module 3 (Intel® RMM3) card. Without the Intel® RMM3, the advanced features are dormant.

4.2.1.1 Intel® Remote Management Module 3 (Intel® RMM3)

The Intel® RMM3 provides the BMC with an additional dedicated network interface. The dedicated interface consumes its own LAN channel. Additionally, the Intel® RMM3 provides additional flash storage for advanced features such as WS-MAN.

4.2.2 Keyboard, Video, and Mouse (KVM) Redirection

The advanced management features include support for keyboard, video, and mouse redirection (KVM) over LAN. This feature is available remotely from the embedded web server

as a Java* applet. The client system must have a Java Runtime Environment (JRE) Version 1.6 (JRE6) or later to run the KVM or media redirection applets. You can download the latest Java Runtime Environment (JRE) update: http://java.com/en/download/index.jsp.

This feature is only enabled when the Intel® RMM3 is present.

Note: KVM Redirection is only available with onboard video controller, and the onboard video controller must be enabled and used as the primary video output.

The BIOS will detect one set of USB keyboard and mouse for the KVM redirection function of Intel® RMM3, even if no presence of RMM3 is detected. Users will see one set of USB keyboard and mouse in addition to the local USB connection on the BIOS Setup USB screen with or without RMM3 installed.

4.2.2.1 Keyboard and Mouse

The keyboard and mouse are emulated by the BMC as USB human interface devices.

4.2.2.2 Video

Video output from the KVM subsystem is equivalent to video output on the local console via onboard video controller. Video redirection is available once video is initialized by the system BIOS. The KVM video resolutions and refresh rates will always match the values set in the operating system.

4.2.2.3 Availability

Up to two remote KVM sessions are supported. An error displays on the web browser attempting to launch more than two KVM sessions.

The default inactivity timeout is 30 minutes, but you may change the default through the embedded web server. Remote KVM activation does not disable the local system keyboard, video, or mouse. Unless the feature is disabled locally, remote KVM is not deactivated by local system input.

KVM sessions will persist across system reset but not across an AC power loss.

4.2.3 Media Redirection

The embedded web server provides a Java* applet to enable remote media redirection. You may use this 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 as a local device to the server, allowing system administrators or users to boot the server or install software (including operating systems), copy files, update the BIOS, and so forth, 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 usable in parallel.
- You can mount either IDE (CD-ROM, floppy) or USB devices 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. For more information, refer to the Tested/supported Operating System List.
- It is possible to mount at least two devices concurrently.
- The mounted device is visible to (and usable by) the managed system's operating system and BIOS in both the pre- 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 operating system present) using the remotely mounted device. This may also require the use of KVM-r to configure the operating system during install.

If either a virtual IDE or virtual floppy device is remotely attached during system boot, both 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.

4.2.3.1 Availability

The default inactivity timeout is 30 minutes and is not user-configurable.

Media redirection sessions persist across system reset but not across an AC power loss.

4.2.4 Web Services for Management (WS-MAN)

The BMC firmware supports the Web Services for Management (WS-MAN) specification, version 1.0.

4.2.4.1 Profiles

The BMC supports the following DMTF profiles for WS-MAN:

- Base Server Profile
- Fan Profile
- Physical Asset Profile
- Power State Management Profile
- Profile Registration Profile
- Record Log Profile
- Sensor Profile
- Software Inventory Profile (FW Version)

Note: WS-MAN features will be made available after production launch.

4.2.5 Embedded Web server

The BMC provides an embedded web server for out-of-band management. User authentication is handled by IPMI user names and passwords. Base functionality for the embedded web server includes:

- Power Control
- Sensor Reading
- SEL Reading
- KVM/Media Redirection: Only available when the Intel® RMM3 is present.
- IPMI User Management

The web server is available on all enabled LAN channels. If a LAN channel is enabled, properly configured, and accessible, the web server is available.

The web server may be contacted via HTTP or HTTPS. A user can modify the SSL certificates using the web server. You cannot change the web server's port (80/81).

For security reasons, you cannot use the null user (user 1) to access the web server. The session inactivity timeout for the embedded web server is 30 minutes. This is not user-configurable.

4.2.6 Lightweight Directory Authentication Protocol (LDAP)

The BMC firmware supports the Linux Lightweight Directory Authentication Protocol (LDAP) protocol for user authentication. IPMI users/passwords and sessions are not supported over LDAP.

A user can configure LDAP usage through the embedded web server for authentication of future embedded web sessions.

Note: Supports LDAP for Linux only.

4.3 Platform Control

This server platform has embedded platform control which is capable of automatically adjusting system performance and acoustic levels.

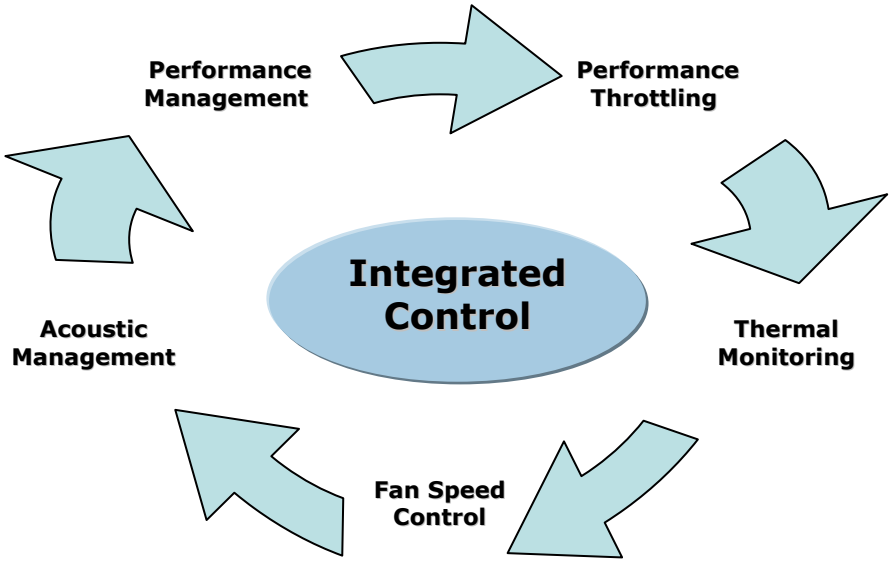


Figure 26. Platform Control

Platform control optimizes system performance and acoustics levels through:

- Performance management
- Performance throttling
- Thermal monitoring
- Fan speed control
- Acoustics management

The platform components used to implement platform control include:

- Integrated baseboard management controller
- Platform sensors
- Variable speed system fans
- System BIOS
- BMC firmware
- Sensor data records as loaded by the FRUSDR Utility
- Memory type

4.3.1 Memory Open and Closed Loop Thermal Throttling

Open-Loop Thermal Throttling (OLTT)
Throttling is a solution to cool the DIMMs by reducing memory traffic allowed on the memory bus, which reduces power consumption and thermal output. With OLTT, the system throttles in response to memory bandwidth demands instead of actual memory temperature. Since there is no direct temperature feedback from the DDR3 DIMMs, the throttling behavior is preset rather than conservatively based on the worst cooling conditions (for example, high inlet temperature and low fan speeds). Additionally, the fans that provide cooling to the memory region are also set to conservative settings (for example, higher minimal fan speed). OLTT produces a slightly louder system than CLTT because minimal fan speeds must be set high enough to support any DDR3 DIMMs in the worst memory cooling conditions.

Closed-Loop Thermal Throttling (CLTT)
CLTT works by throttling the DDR3 DIMMs response directly to memory temperature via thermal sensors integrated on the Serial Presence Detect (SPD) of the DDR3 DIMMs. This is the preferred throttling method because this approach lowers limitations on both memory power and thermal threshold, therefore minimizing throttling impact on memory performance. This reduces the utilization of high fan speeds because CLTT does not have to accommodate for the worst memory cooling conditions; with a higher thermal threshold, CLTT enables memory performance to achieve optimal levels.

4.3.2 Fan Speed Control

BIOS and BMC software work cooperatively to implement system thermal management support. During normal system operation, the BMC will retrieve information from the BIOS and monitor several platform thermal sensors to determine the required fan speeds.

In order to provide the proper fan speed control for a given system configuration, the BMC must have the appropriate platform data programmed. Platform configuration data is programmed using the FRUSDR utility during the system integration process and by System BIOS during run time.

4.3.2.1 System Configuration Using the FRUSDR Utility

The Field Replaceable Unit and Sensor Data Record Update Utility (FRUSDR utility) is a program used to write platform-specific configuration data to NVRAM on the server board. It allows the user to select which supported chassis (Intel or Non-Intel) and platform chassis configuration is used. Based on the input provided, the FRUSDR writes sensor data specific to the configuration to NVRAM for the BMC controller to read each time the system is powered on.

4.3.2.2 Fan Speed Control from BMC and BIOS Inputs

Using the data programmed to NVRAM by the FRUSDR utility, the BMC is configured to monitor and control the appropriate platform sensors and system fans each time the system is powered on. After power-on, the BMC uses additional data provided to it by the System BIOS to determine how to control the system fans.

The BIOS provides data to the BMC telling it which fan profile the platform is set up for: Acoustics Mode or Performance Mode. The BIOS uses the parameters retrieved from the thermal sensor data records (SDR), fan profile setting from BIOS Setup, and altitude setting from the BIOS Setup to configure the system for memory throttling and fan speed control. If the

BIOS fails to get the Thermal SDRs, then it uses the Memory Reference Code (MRC) default settings for the memory throttling settings.

The <F2> BIOS Setup Utility provides options to set the fan profile or operating mode the platform will operate under. Each operating mode has a predefined profile for which specific platform targets are configured, which in turn determines how the system fans operate to meet those targets. Platform profile targets are determined by which type of platform is selected when running the FRUSDR utility and by the BIOS settings configured using the <F2> BIOS Setup.

4.3.2.2.1 Fan Domains

System fan speeds are controlled through pulse width modulation (PWM) signals, which are driven separately for each domain by integrated PWM hardware. Fan speed is changed by adjusting the duty-cycle, which is the percentage of time the signal is driven high in each pulse. Refer to Appendix D for system specific fan domains.

Table 18. S5520HC, S5500HCV and S5520HCT Fan Domain Table

Fan Domain	Onboard Fan Header
Fan Domain 0	CPU 1 Fan, CPU 2 Fan
Fan Domain 1	System Fan 5
Fan Domain 2	System Fan 1, System Fan 2
Fan Domain 3	System Fan 3, System Fan 4

4.3.2.3 Configuring the Fan Profile Using the BIOS Setup Utility

The BIOS uses options set in the <F2> BIOS Setup Utility to determine what fan profile the system should operate under. These options include “THROTTLING MODE”, “ALTITUDE”, and “SET FAN PROFILE”. Refer to “*Section 5.3.2.2.7 System Acoustic and Performance Configuration*” for details of the BIOS options.

The “ALTITUDE” option is used to determine appropriate memory performance settings based on the different cooling capability at different altitudes. At high altitude, memory performance must be reduced to compensate for thinner air. Be advised, selecting an Altitude option to a setting that does not meet the operating altitude of the server may limit the system fans’ ability to provide adequate cooling to the memory. If the air flow is not sufficient to meet the needs of the server even after throttling has occurred, the system may shut down due to excessive platform thermals.

By default, the Altitude option is set to 301 m – 900 m which is believed to cover the majority of the operating altitudes for these server platforms.

You can set the “SET FAN PROFILE” option to either the Performance mode (Default) or Acoustics mode. Refer to the following sections for details describing the differences between each mode. Changing the fan profile to Acoustics mode may affect system performance. The “SET FAN PROFILE” BIOS option is hidden when CLTT is selected as the THROTTLING MODE option.

4.3.2.3.1 Performance Mode (Default)

With the platform running in Performance mode (Default), several platform control algorithm variables are set to enhance the platform’s capability of operating at maximum performance targets for the given system. In doing so, the platform is programmed with higher fan speeds at lower ambient temperatures. This results in a louder acoustic level than is targeted for the given

platform, but the increased airflow of this operating mode greatly reduces both possible memory throttling from occurring and dynamic fan speed changes based on processor utilization.

4.3.2.3.2 Acoustics Mode

With the platform running in Acoustics mode, several platform control algorithm variables are set to ensure acoustic targets are not exceeded for specified Intel platforms. In this mode, the platform is programmed to set the fans at lower speeds when the processor does not require additional cooling due to high utilization/power consumption. Memory throttling is used to ensure memory thermal limits are not exceeded.

Note: Fan speed control for a non-Intel chassis, as configured after running the FRUSDR utility and selecting the Non-Intel Chassis option, is limited to only the CPU fans. The BMC only requires the processor thermal sensor data to determine how fast to operate these fans. The remaining system fans will operate at 100% operating limits due to unknown variables associated with the given chassis and its fans. Therefore, regardless of whether the system is configured for Performance Mode or Acoustics Mode, the system fans will always run at 100% operating levels providing for maximum airflow. In this scenario, the Performance and Acoustic mode settings only affect the allowable performance of the memory (higher BW for the Performance mode).

4.4 Intel® Intelligent Power Node Manager

Intel® Intelligent Power Node Manager is a platform (system)-level solution that provides the system with a method of monitoring power consumption and thermal output, and adjusting system variables to control those factors.

The BMC supports Intel® Intelligent Power Node Manager specification version 1.5. Additionally, the platform must have an Intel® Intelligent Power Node Manager capable Manageability Engine (ME) firmware installed.

The BMC firmware implements power-management features based on the *Power Management Bus (PMBus) 1.1 Specification*.

Note: Intelligent Power Node Manager is only available on platforms that support PMBus-compliant power supplies.

4.4.1 Manageability Engine (ME)

An embedded ARC controller is within the IOH providing the Intel® Server Platform Services (SPS). The controller is also commonly referred to as the Manageability Engine (ME).

The functionality provided by the SPS firmware is different from Intel® Active Management Technology (Intel® AMT) provided by the ME on client platforms.

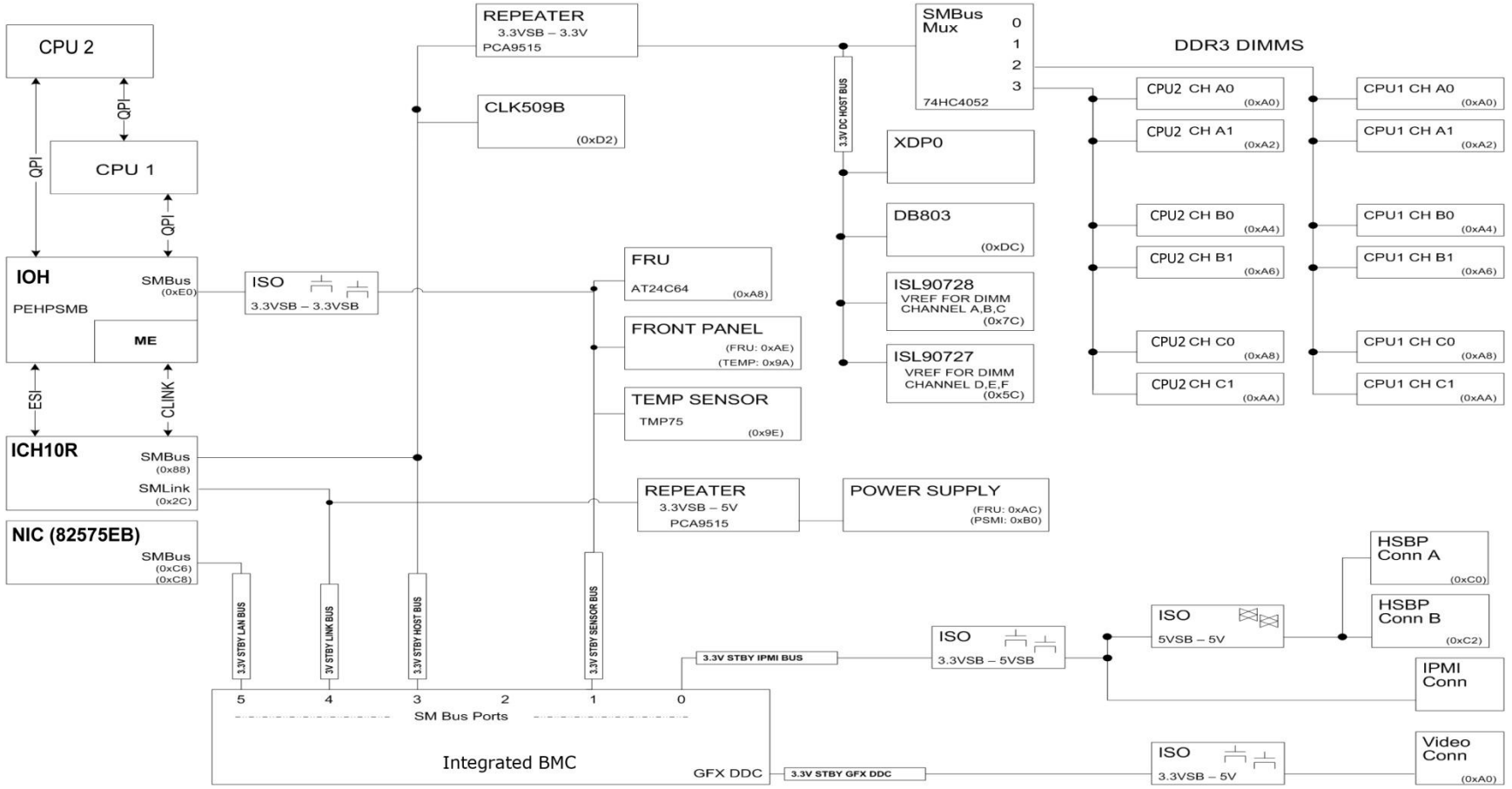


Figure 27. SMBUS Block Diagram

5. BIOS Setup Utility

5.1 Logo/Diagnostic Screen

The Logo/Diagnostic Screen displays in one of two forms:

- If Quiet Boot is enabled in the BIOS setup, a logo splash screen is displayed. By default, Quiet Boot is enabled in the BIOS setup. If the logo displays during POST, press <Esc> to hide the logo and display the diagnostic screen.
- If a logo is not present in the flash ROM or if Quiet Boot is disabled in the system configuration, the summary and diagnostic screen is displayed.

The diagnostic screen displays the following information:

- BIOS ID
- Platform name
- Total memory detected (Total size of all installed DDR3 DIMMs)
- Processor information (Intel branded string, speed, and number of physical processors identified)
- Keyboards detected (if plugged in)
- Mouse devices detected (if plugged in)

5.2 BIOS Boot Popup Menu

The BIOS Boot Specification (BBS) provides for a Boot Popup Menu invoked by pressing the <F6> key during POST. The BBS popup menu displays all available boot devices. The list order in the popup menu is not the same as the boot order in the BIOS setup; it simply lists all the bootable devices from which the system can be booted.

When a User Password or Administrator Password is active in Setup, the password is to access the Boot Popup Menu.

5.3 BIOS Setup Utility

The BIOS Setup utility is a text-based utility that allows the user to configure the system and view current settings and environment information for the platform devices. The Setup utility controls the platform's built-in devices, boot manager, and error manager.

The BIOS Setup interface consists of a number of pages or screens. Each page contains information or links to other pages. The advanced tab in Setup displays a list of general categories as links. These links lead to pages containing a specific category’s configuration.

The following sections describe the look and behavior for platform setup.

5.3.1 Operation

The BIOS Setup has the following features:

- Localization - The BIOS Setup uses the Unicode standard and is capable of displaying setup forms in all languages currently included in the Unicode standard. The Intel® server board BIOS is only available in English.
- Console Redirection - The BIOS Setup is functional via console redirection over various terminal emulation standards. This may limit some functionality for compatibility (for example, color usage or some keys or key sequences or support of pointing devices).

5.3.1.1 Setup Page Layout

The setup page layout is sectioned into functional areas. Each occupies a specific area of the screen and has dedicated functionality. The following table lists and describes each functional area.

Table 19. BIOS Setup Page Layout

Functional Area	Description
Title Bar	The title bar is located at the top of the screen and displays the title of the form (page) the user is currently viewing. It may also display navigational information.
Setup Item List	The Setup Item List is a set of controllable and informational items. Each item in the list occupies the left column of the screen. A Setup Item may also open a new window with more options for that functionality on the board.
Item Specific Help Area	The Item Specific Help area is located on the right side of the screen and contains help text for the highlighted Setup Item. Help information may include the meaning and usage of the item, allowable values, effects of the options, and so forth.
Keyboard Command Bar	The Keyboard Command Bar is located at the bottom right of the screen and continuously displays help for keyboard special keys and navigation keys.

5.3.1.2 Entering BIOS Setup

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. However, serious errors cause the system to display the Error Manager screen instead of the Main screen.

5.3.1.3 Keyboard Commands

The bottom right portion of the Setup screen provides a list of commands used to navigate through the Setup utility. These commands display at all times.

Each Setup menu page contains a number of features. Each feature is associated with a value field except those used for informative purposes. Each value field contains configurable parameters. Depending on the security option selected and in effect by the password, a menu feature's value may or may not change. If a value cannot be changed, its field is made inaccessible and appears grayed out.

Table 20. BIOS Setup: Keyboard Command Bar

Key	Option	Description
<Enter>	Execute Command	The <Enter> key is used to activate sub-menus when the selected feature is a sub-menu, or to display a pick list if a selected option has a value field, or to select a sub-field for multi-valued features like time and date. If a pick list is displayed, the <Enter> key selects the currently highlighted item, undoes the pick list, and returns the focus to the parent menu.
<Esc>	Exit	The <Esc> key provides a mechanism for backing out of any field. When the <Esc> key is pressed while editing any field or selecting features of a menu, the parent menu is re-entered. When the <Esc> key is pressed in any sub-menu, the parent menu is re-entered. When the <Esc> key is pressed in any major menu, the exit confirmation window is displayed and the user is asked whether changes can be discarded. If “No” is selected and the <Enter> key is pressed, or if the <Esc> key is pressed, the user is returned to where they were before <Esc> was pressed, without affecting any existing settings. If “Yes” is selected and the <Enter> key is pressed, the setup is exited and the BIOS returns to the main System Options Menu screen.
↑	Select Item	The up arrow is used to select the previous value in a pick list, or the previous option in a menu item's option list. The selected item must then be activated by pressing the <Enter> key.
↓	Select Item	The down arrow is used to select the next value in a menu item’s option list, or a value field’s pick list. The selected item must then be activated by pressing the <Enter> key.
↔	Select Menu	The left and right arrow keys are used to move between the major menu pages. The keys have no effect if a sub-menu or pick list is displayed.
<Tab>	Select Field	The <Tab> key is used to move between fields. For example, you can use <Tab> to move from hours to minutes in the time item in the main menu.
-	Change Value	The minus key on the keypad is used to change the value of the current item to the previous value. This key scrolls through the values in the associated pick list without displaying the full list.
+	Change Value	The plus key on the keypad is used to change the value of the current menu item to the next value. This key scrolls through the values in the associated pick list without displaying the full list. On 106-key Japanese keyboards, the plus key has a different scan code than the plus key on the other keyboards, but will have the same effect.
<F9>	Setup Defaults	Pressing <F9> causes the following to display: **Load Optimized Defaults?** **Yes No** If “Yes” is highlighted and <Enter> is pressed, all Setup fields are set to their default values. If “No” is highlighted and <Enter> is pressed, or if the <Esc> key is pressed, the user is returned to where they were before <F9> was pressed without affecting any existing field values.
<F10>	Save and Exit	Pressing <F10> causes the following message to display: **Save configuration and reset?** **Yes No** If “Yes” is highlighted and <Enter> is pressed, all changes are saved and the Setup is exited. If “No” is highlighted and <Enter> is pressed, or the <Esc> key is pressed, the user is returned to where they were before <F10> was pressed without affecting any existing values.

5.3.1.4 Menu Selection Bar

The Menu Selection Bar is located at the top of the BIOS Setup Utility screen. It displays the major menu selections available to the user. By using the left and right arrow keys, the user can select the menus listed here. Some menus are hidden and become available by scrolling off the left or right of the current selections.

5.3.2 Server Platform Setup Utility Screens

The following sections describe the screens available for the configuration of a server platform. In these sections, tables are used to describe the contents of each screen. These tables follow the following guidelines:

- The Setup Item, Options, and Help Text columns in the tables document the text and values that also display on the BIOS Setup screens.
- **I**n the Options column, the default values are displayed in bold. These values are not displayed in bold on the BIOS Setup screen. The bold text in this document serves as a reference point.
- The Comments column provides additional information where it may be helpful. This information does not display on the BIOS Setup screens.
- Information enclosed in angular brackets (< >) in the screen shots identifies text that can vary, depending on the option(s) installed. For example <Current Date> is replaced by the actual current date.
- Information enclosed in square brackets ([ ]) in the tables identifies areas where the user must type in text instead of selecting from a provided option.
- Whenever information is changed (except Date and Time), the systems requires a save and reboot to take place. Pressing <ESC> discards the changes and boots the system according to the boot order set from the last boot.

5.3.2.1 Main Screen

Unless an error occurred, the Main screen is the first screen displayed when the BIOS Setup is entered. If an error occurred, the Error Manager screen displays instead.

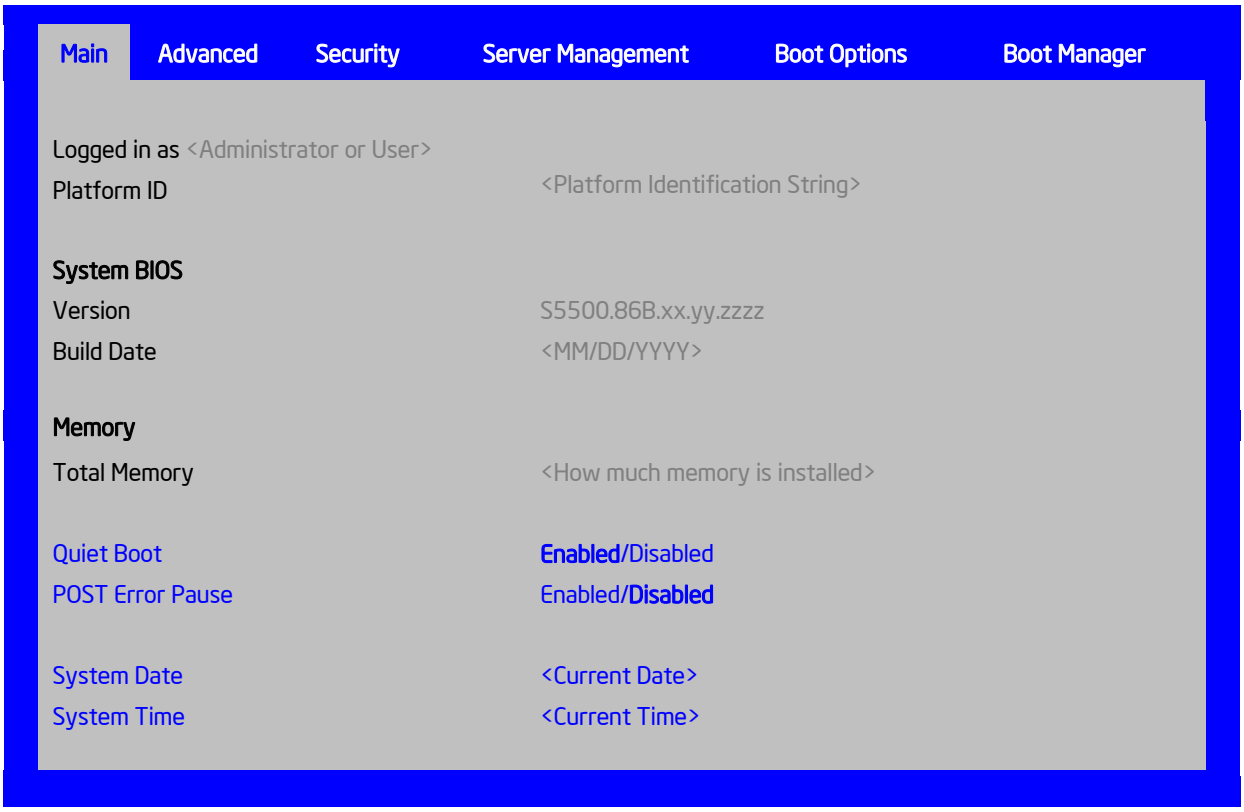


Figure 28. Setup Utility — Main Screen Display

Table 21. Setup Utility — Main Screen Fields

Setup Item	Options	Help Text	Comments
Logged in as			**Information only.** Displays password level that setup is running in: Administrator or User. With no passwords set, Administrator is the default mode.
Platform ID			**Information only.** Displays the Platform ID.
System BIOS			
Version			**Information only.** Displays the current BIOS version. xx = major version yy = minor version zzzz = build number
Build Date			**Information only.** Displays the current BIOS build date.
Memory			

Setup Item	Options	Help Text	Comments
Size			**Information only.** Displays the total physical memory installed in the system, in MB or GB. The term physical memory indicates the total memory discovered in the form of installed DDR3 DIMMs.
Quiet Boot	**Enabled** Disabled	[Enabled] – Display the logo screen during POST. [Disabled] – Display the diagnostic screen during POST.	
POST Error Pause	Enabled **Disabled**	[Enabled] – Go to the Error Manager for critical POST errors. [Disabled] – Attempt to boot and do not go to the Error Manager for critical POST errors.	If enabled, the POST Error Pause option takes the system to the error manager to review the errors when major errors occur. Minor and fatal error displays are not affected by this setting.
System Date	[Day of week MM/DD/YYYY]	System Date has configurable fields for Month, Day, and Year. Use [Enter] or [Tab] key to select the next field. Use [+] or [-] key to modify the selected field.	
System Time	[HH:MM:SS]	System Time has configurable fields for Hours, Minutes, and Seconds. Hours are in 24-hour format. Use [Enter] or [Tab] key to select the next field. Use [+] or [-] key to modify the selected field.	

5.3.2.2 Advanced Screen

The Advanced screen provides an access point to configure several options. On this screen, the user selects the option they must configure. Configurations are performed on the selected screen and not directly on the Advanced screen.

To access this screen from the Main screen, press the right arrow until the Advanced screen is selected.

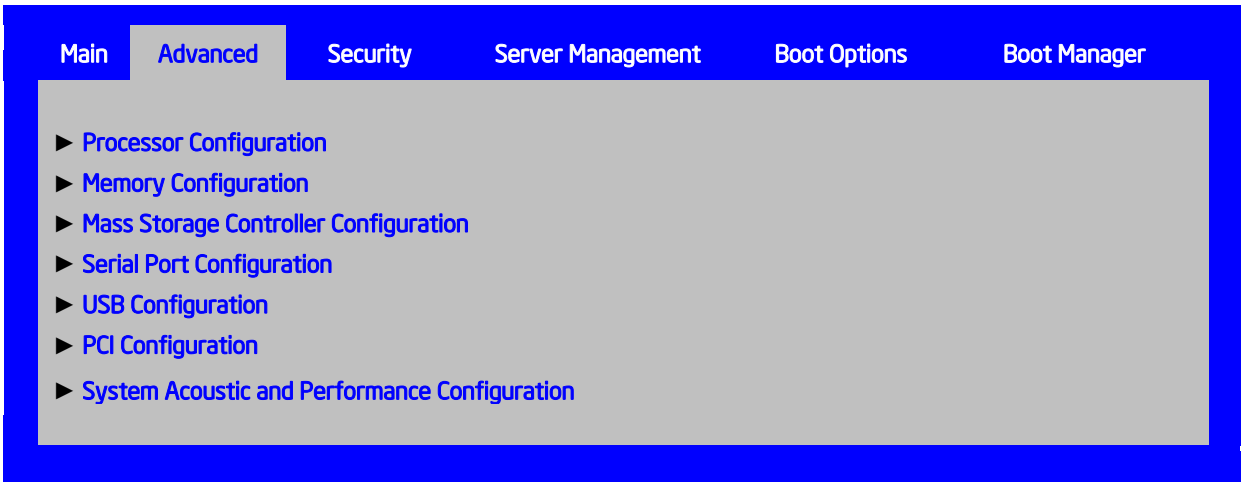


Figure 29. Setup Utility — Advanced Screen Display

Table 22. Setup Utility — Advanced Screen Display Fields

Setup Item	Help Text
Processor Configuration	View/Configure processor information and settings.
Memory Configuration	View/Configure memory information and settings.
Mass Storage Controller Configuration	View/Configure mass storage controller information and settings.
Serial Port Configuration	View/Configure serial port information and settings.
USB Configuration	View/Configure USB information and settings.
PCI Configuration	View/Configure PCI information and settings.
System Acoustic and Performance Configuration	View/Configure system acoustic and performance information and settings.

5.3.2.2.1 Processor Configuration Screen

The Processor screen allows the user to view the processor core frequency, system bus frequency, and to enable or disable several processor options. This screen also allows the user to view information about a specific processor. To access this screen from the Main screen, select **Advanced** > **Processor**.

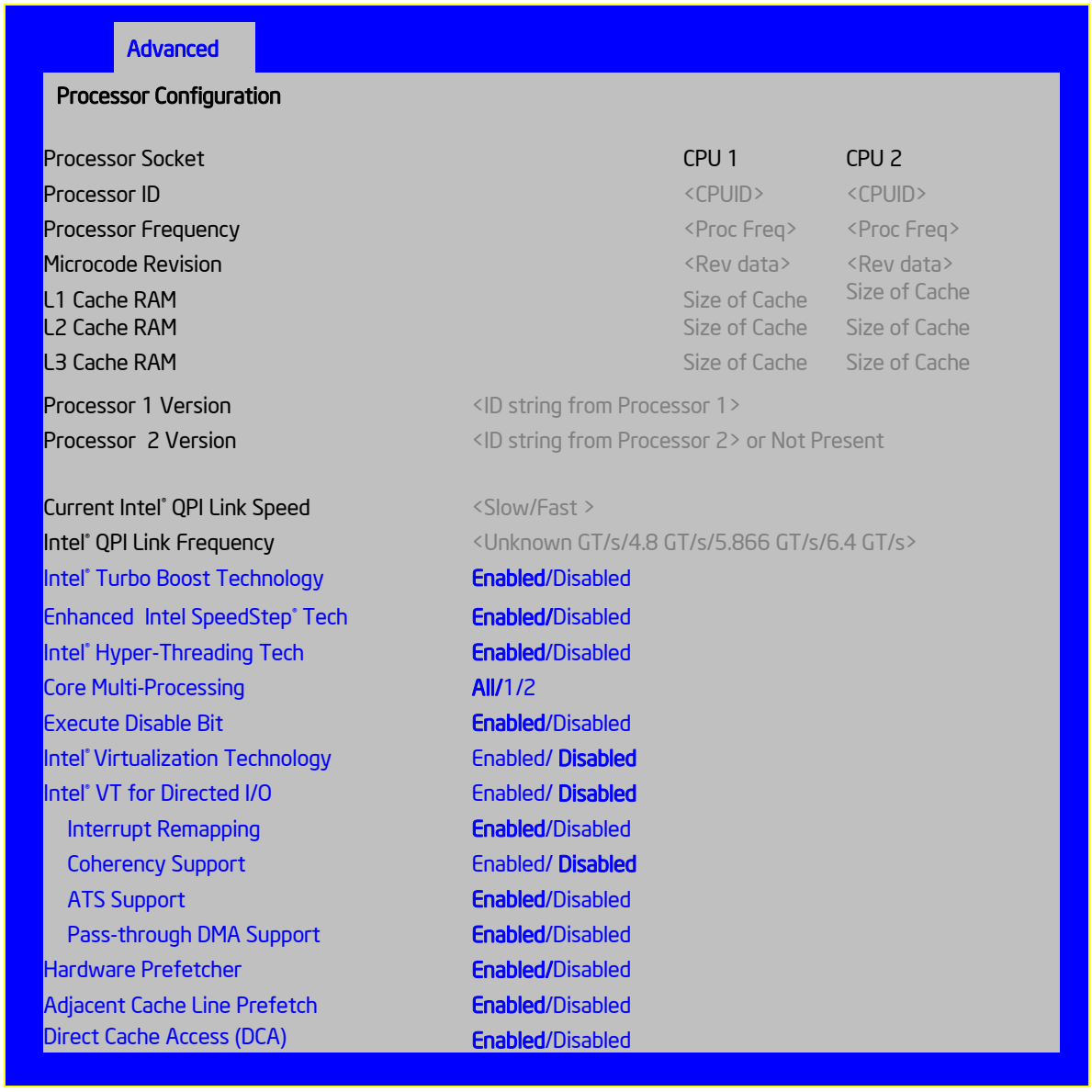


Figure 30. Setup Utility — Processor Configuration Screen Display

Table 23. Setup Utility — Processor Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Processor ID			**Information only.** Processor CPUID
Processor Frequency			**Information only.** Current frequency of the processor.
Microcode Revision			**Information only.** Revision of the loaded microcode.
L1 Cache RAM			**Information only.** Size of the Processor L1 Cache.
L2 Cache RAM			**Information only.** Size of the Processor L2 Cache
L3 Cache RAM			**Information only.** Size of the Processor L3 Cache.
Processor 1 Version			**Information only.** ID string from the Processor.
Processor 2 Version			**Information only.** ID string from the Processor.
Current Intel® QPI Link Speed			**Information only.** Current speed that the QPI Link is using.
Intel® QPI Link Frequency			**Information only.** Current frequency that the QPI Link is using.
Intel® Turbo Boost Technolgy	**Enabled** Disabled	Intel® Turbo Boost Technology allows the processor to automatically increase its frequency if it is running below power, temperature, and current specifications.	This option is only visible if all processors in the system support Intel® Turbo Boost Technology.
Enhanced Intel SpeedStep® Tech	**Enabled** Disabled	Enhanced Intel SpeedStep® Technology allows the system to dynamically adjust processor voltage and core frequency, which can result in decreased average power consumption and decreased average heat production. Contact your OS vendor regarding OS support of this feature.	
Intel® Hyper-Threading Tech	**Enabled** Disabled	Intel® HT Technology allows multithreaded software applications to execute threads in parallel within each processor. Contact your OS vendor regarding OS support of this feature.	
Core Multi-Processing	**All** 1 2	Enable 1, 2 or All cores of installed processors packages.	
Execute Disable Bit	**Enabled** Disabled	Execute Disable Bit can help prevent certain classes of malicious buffer overflow attacks. Contact your OS vendor regarding OS support of this feature.	
Intel® Virtualization Technology	Enabled **Disabled**	Intel® Virtualization Technology allows a platform to run multiple operating systems and applications in independent partitions. **Note**: A change to this option requires the system to be powered off and then back on before the setting takes effect.	

Setup Item	Options	Help Text	Comments
Intel® Virtualization Technology for Directed I/O	Enabled **Disabled**	Enable/Disable Intel® Virtualization Technology for Directed I/O. Report the I/O device assignment to VMM through DMAR ACPI Tables	
Interrupt Remapping	**Enabled** Disabled	Enable/Disable Intel® VT-d Interrupt Remapping support.	Only appears when Intel® Virtualization Technology for Directed I/O is enabled.
Coherency Support	Enabled **Disabled**	Enable/Disable Intel® VT-d Coherency support.	Only appears when Intel® Virtualization Technology for Directed I/O is enabled.
ATS Support	**Enabled** Disabled	Enable/Disable Intel® VT-d Address Translation Services (ATS) support.	Only appears when Intel® Virtualization Technology for Directed I/O is enabled.
Pass-through DMA Support	**Enabled** Disabled	Enable/Disable Intel® VT-d Pass-through DMA support.	Only appears when Intel® Virtualization Technology for Directed I/O is enabled.
Hardware Prefetcher	**Enabled** Disabled	Hardware Prefetcher is a speculative prefetch unit within the processor(s). **Note**: Modifying this setting may affect system performance.	
Adjacent Cache Line Prefetch	**Enabled** Disabled	[Enabled] - Cache lines are fetched in pairs (even line + odd line). [Disabled] - Only the current cache line required is fetched. **Note**: Modifying this setting may affect system performance.	
Direct Cache Access (DCA)	**Enabled** Disabled	Allows processors to increase the I/O performance by placing data from I/O devices directly into the processor cache.	

5.3.2.2.2 Memory Screen

The Memory screen allows the user to view details about the system memory DDR3 DIMMs installed. This screen also allows the user to open the Configure Memory RAS and Performance screen.

To access this screen from the Main screen, select **Advanced** > **Memory**.

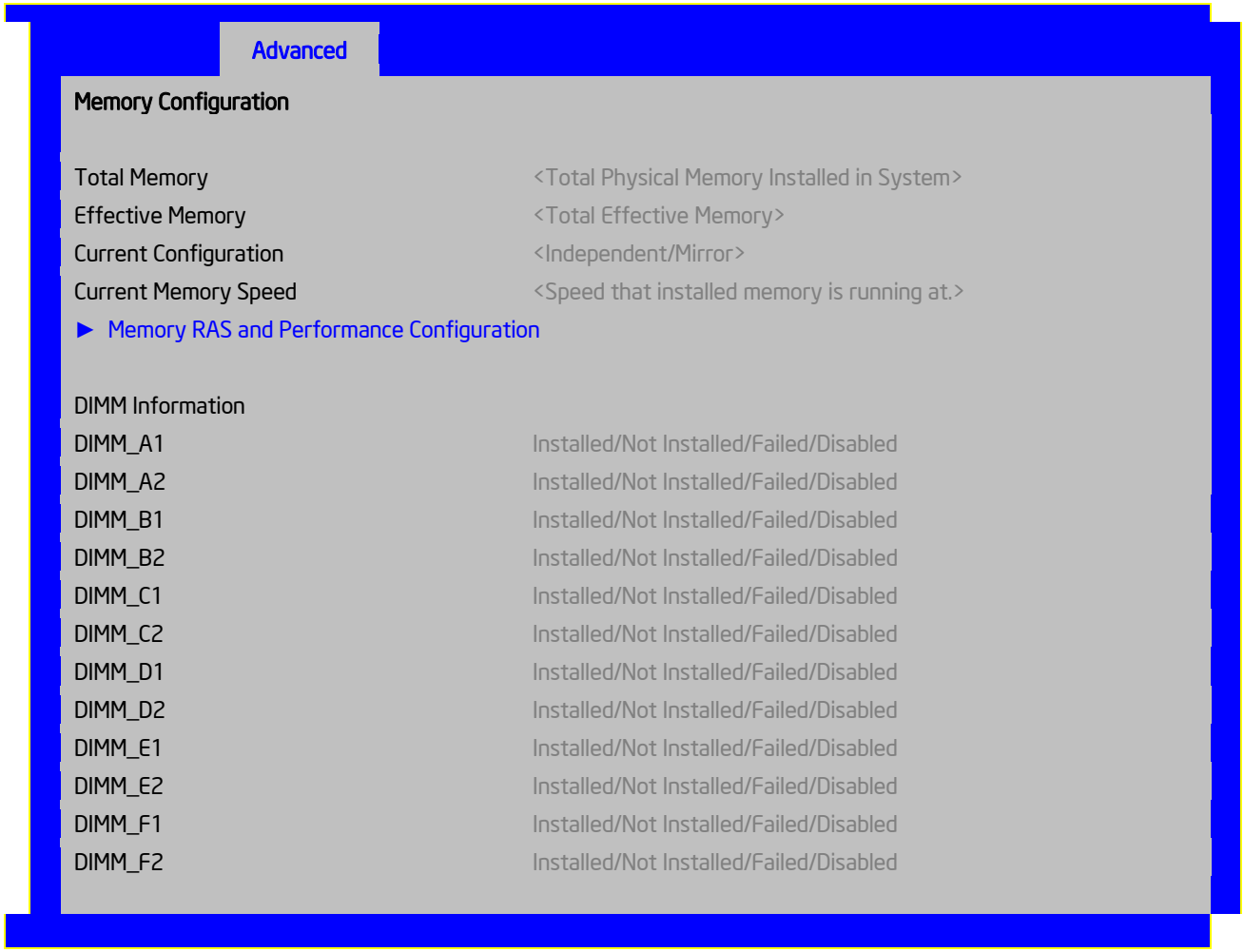


Figure 31. Setup Utility — Memory Configuration Screen Display

Table 24. Setup Utility — Memory Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Total Memory			**Information only.** The amount of memory available in the system in the form of installed DDR3 DIMMs in units of MB or GB.
Effective Memory			**Information only.** The amount of memory available to the operating system in MB or GB. The Effective Memory is the difference between Total Physical Memory and the sum of all memory reserved for internal usage, RAS redundancy and SMRAM. This difference includes the sum of all DDR3 DIMMs that failed Memory BIST during POST, or were disabled by the BIOS during memory discovery phase in order to optimize memory configuration.
Current Configuration			**Information only.** Displays one of the following: – **Independent Mode:** System memory is configured for optimal performance and efficiency and no RAS is enabled. – **Mirror Mode:** System memory is configured for maximum reliability in the form of memory mirroring.
Current Memory Speed			**Information only.** Displays the speed the memory is running at.
Memory RAS and Performance Configuration		Configure memory RAS (Reliability, Availability, and Serviceability) and view current memory performance information and settings.	Select to configure the memory RAS and performance. This takes the user to a different screen.
DIMM_ XY			Displays the state of each DIMM socket present on the board. Each DIMM socket field reflects one of the following possible states: – **Installed:** There is a DDR3 DIMM installed in this slot. – **Not Installed:** There is no DDR3 DIMM installed in this slot. – **Disabled:** The DDR3 DIMM installed in this slot was disabled by the BIOS to optimize memory configuration. – **Failed:** The DDR3 DIMM installed in this slot is faulty/malfunctioning. **Note:** X denotes the Channel Identifier and Y denote the DIMM Identifier within the Channel.

5.3.2.2.2.1 Configure Memory RAS and Performance Screen

The Configure Memory RAS and Performance screen allows the user to customize several memory configuration options, such as whether to use Memory Mirroring.

To access this screen from the Main screen, select **Advanced** > **Memory** > **Configure Memory RAS and Performance**.

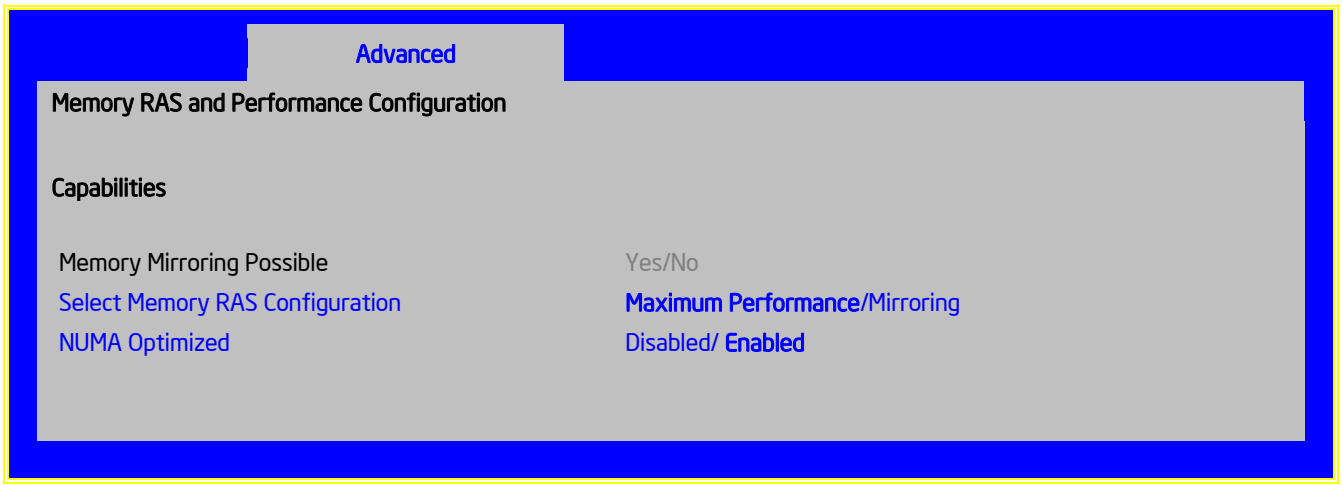


Figure 32. Setup Utility — Configure RAS and Performance Screen Display

Table 25. Setup Utility — Configure RAS and Performance Screen Fields

Setup Item	Options	Help Text	Comments
Memory Mirroring Possible	Yes/No		**Information only.** Only displayed on systems with chipsets capable of Memory Mirroring.
Select Memory RAS Configuration	**Maximum Performance** Mirroring	Available modes depend on the current memory population. [**Maximum Performance**] - Optimizes system performance. [**Mirroring**] - Optimizes reliability by using half of physical memory as a backup.	Only available if Mirroring is possible.
NUMA Optimized	**Enabled** Disabled	If enabled, BIOS includes ACPI tables that are required for NUMA aware Operating Systems.	

5.3.2.2.3 Mass Storage Controller Screen

The Mass Storage screen allows the user to configure the SATA/SAS controller when it is present on the baseboard module card of an Intel system.

To access this screen from the Main menu, select **Advanced** > **Mass Storage**.

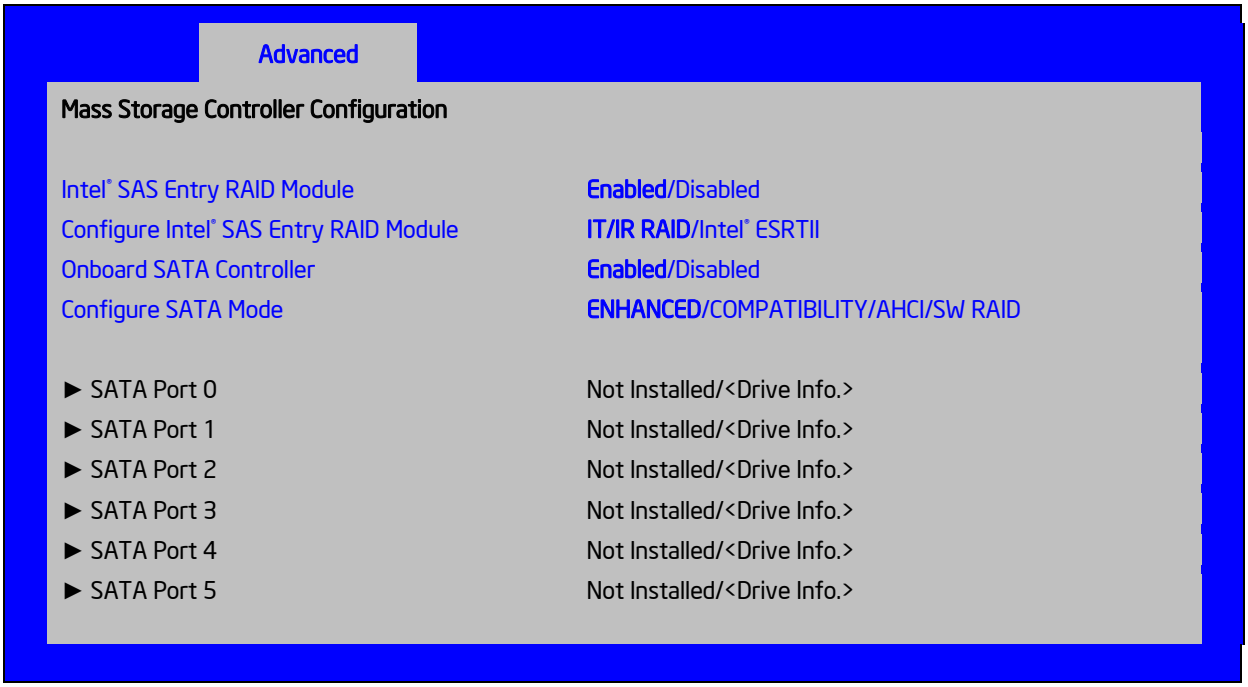


Figure 33. Setup Utility — Mass Storage Controller Configuration Screen Display

Table 26. Setup Utility — Mass Storage Controller Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Intel® Entry SAS RAID Module	**Enabled** Disabled	Enabled or Disable the Intel® SAS Entry RAID Module	Unavailable if the SAS Module (AXX4SASMOD) is not present.
Configure Intel® Entry SAS RAID Module	**IT/IR RAID** Intel® ESRTII	IT/IR RAID – Supports Entry-Level HW RAID 0, RAID 1, and RAID 1e, as well as native SAS pass through mode; Intel® ESRTII - Intel® Embedded Server RAID Technology II, which supports RAID 0, RAID 1, RAID 10 and RAID 5 mode. RAID 5 support requires optional Software RAID 5 Activation Key	Unavailable if the SAS Module (AXX4SASMOD) is disabled or not present.
Onboard SATA Controller	**Enabled** Disabled	Onboard Serial ATA (SATA) controller.	
SATA Mode	**Enhanced** Compatibility AHCI SW RAID	[ENHANCED] - Supports up to 6 SATA ports with IDE Native Mode. [COMPATIBILITY] - Supports up to 4 SATA ports[0/1/2/3] with IDE Legacy mode and 2 SATA ports[4/5] with IDE Native Mode. [AHCI] - Supports all SATA ports using the Advanced Host Controller Interface. [SW RAID] - Supports configuration of SATA ports for RAID via RAID configuration software.	No longer displays when the Onboard SATA Controller is disabled. Changing this setting requires a reboot before you can set the HDD boot order. [SW RAID] option is unavailable when EFI Optimized Boot is Enabled. SW RAID can only be used in Legacy Boot mode.
SATA Port 0	< Not Installed/Drive information>		**Information only.** This field is unavailable when RAID Mode is enabled.
SATA Port 1	< Not Installed/Drive information>		**Information only.** This field is unavailable when RAID Mode is enabled.
SATA Port 2	< Not Installed/Drive information>		**Information only.** This field is unavailable when RAID Mode is enabled.
SATA Port 3	< Not Installed/Drive information>		**Information only.** This field is unavailable when RAID Mode is enabled.
SATA Port 4	< Not Installed/Drive information>		**Information only.** This field is unavailable when RAID Mode is enabled.
SATA Port 5	< Not Installed/Drive information>		**Information only.** This field is unavailable when RAID Mode is enabled.

5.3.2.2.4 Serial Ports Screen

The Serial Ports screen allows the user to configure the Serial A [COM 1] and Serial B [COM2] ports.

To access this screen from the Main screen, select **Advanced** > **Serial Port**.

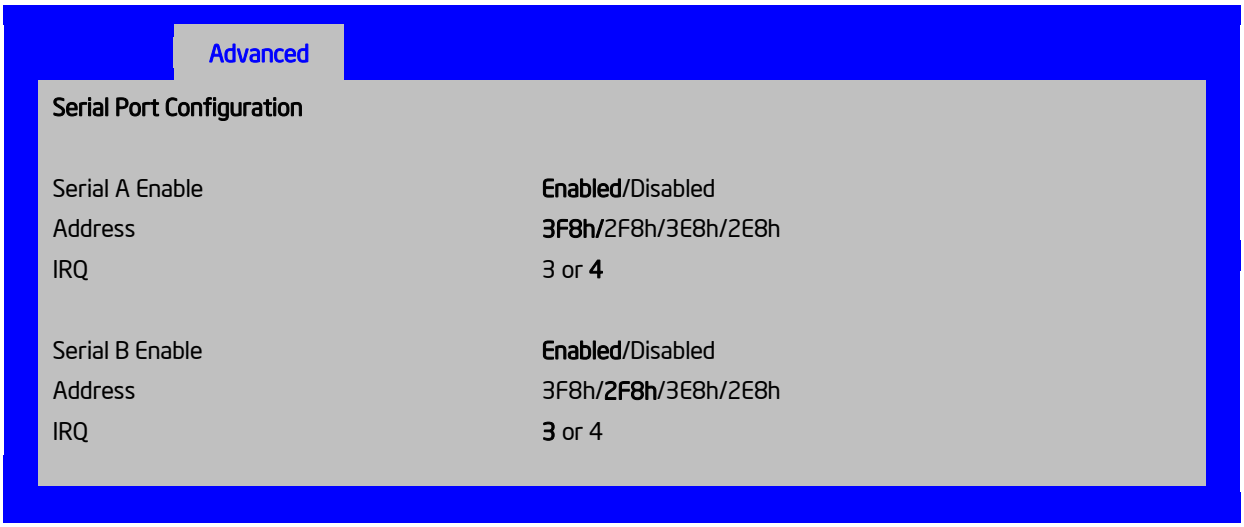


Figure 34. Setup Utility — Serial Port Configuration Screen Display

Table 27. Setup Utility — Serial Ports Configuration Screen Fields

Setup Item	Options	Help Text
Serial A Enable	**Enabled** Disabled	Enable or Disable Serial port A.
Address	**3F8h** 2F8h 3E8h 2E8h	Select Serial port A base I/O address.
IRQ	3 **4**	Select Serial port A interrupt request (IRQ) line.
Serial B Enable	**Enabled** Disabled	Enable or Disable Serial port B.
Address	3F8h **2F8h** 3E8h 2E8h	Select Serial port B base I/O address.
IRQ	**3** 4	Select Serial port B interrupt request (IRQ) line.

5.3.2.2.5 USB Configuration Screen

The USB Configuration screen allows the user to configure the USB controller options.

To access this screen from the Main screen, select **Advanced** > **USB Configuration**.

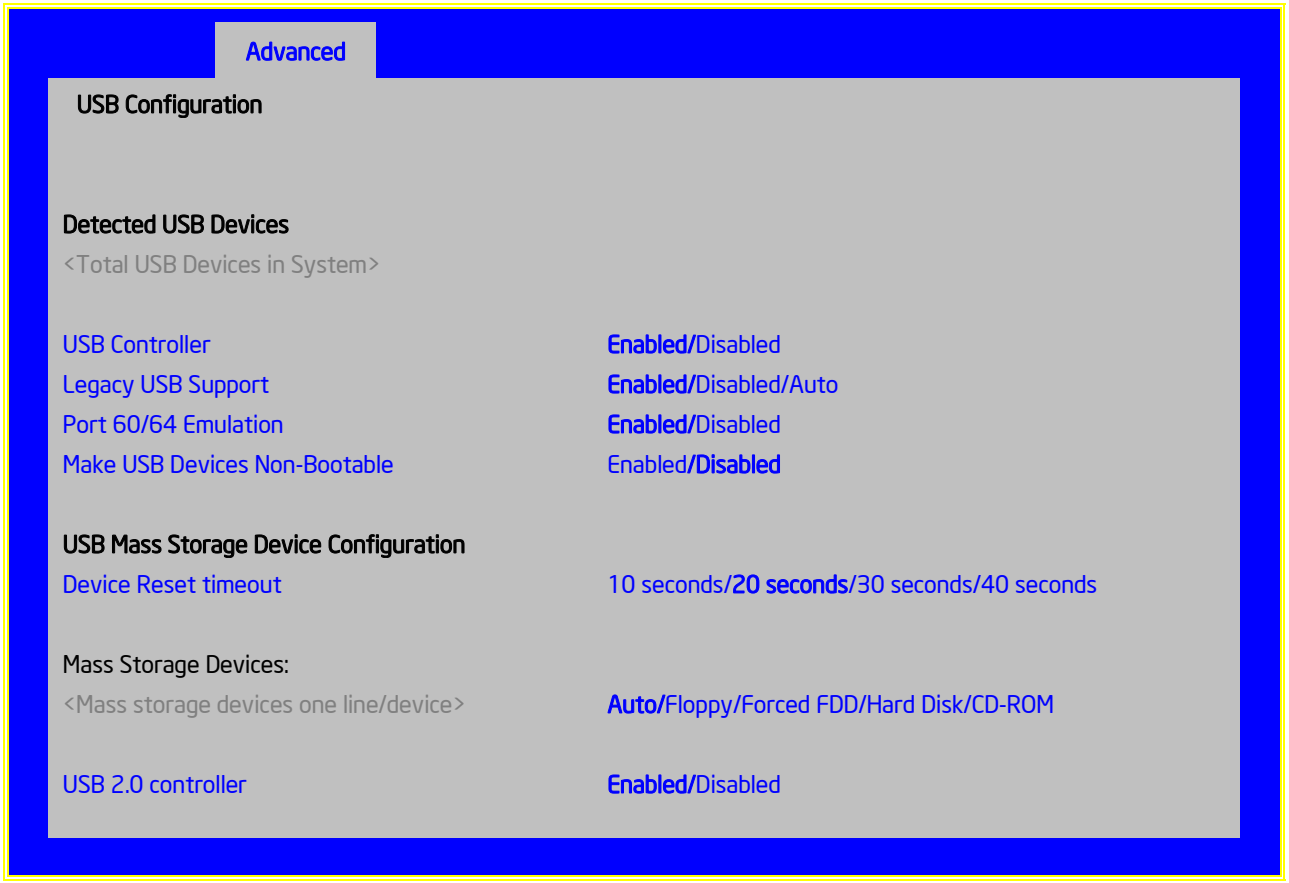


Figure 35. Setup Utility — USB Controller Configuration Screen Display

Table 28. Setup Utility — USB Controller Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Detected USB Devices			**Information only.** Shows the number of USB devices in the system.
USB Controller	**Enabled** Disabled	[Enabled] - All onboard USB controllers are turned on and accessible by the OS. [Disabled] - All onboard USB controllers are turned off and inaccessible by the OS.	
Legacy USB Support	**Enabled** Disabled Auto	USB device boot support and PS/2 emulation for USB keyboard and USB mouse devices. [Auto] - Legacy USB support is enabled if a USB device is attached.	Grayed out if the USB Controller is disabled.
Port 60/64 Emulation	**Enabled** Disabled	I/O port 60h/64h emulation support. **Note**: This may be needed for legacy USB keyboard support when using an OS that is USB unaware.	Grayed out if the USB Controller is disabled.
Make USB Devices Non-Bootable	Enabled **Disabled**	Exclude USB in Boot Table. [Enabled] - This removes all USB Mass Storage devices as Boot options. [Disabled] - This allows all USB Mass Storage devices as Boot options.	Grayed out if the USB Controller is disabled.
Device Reset timeout	10 sec **20 sec** 30 sec 40 sec	USB Mass Storage device Start Unit command timeout. Setting to a larger value provides more time for a mass storage device to be ready, if needed.	Grayed out if the USB Controller is disabled.
One line for each mass storage device in system	**Auto** Floppy Forced FDD Hard Disk CD-ROM	[Auto] - USB devices less than 530 MB are emulated as floppies. [Forced FDD] - HDD formatted drive are emulated as a FDD (e.g., ZIP drive).	Hidden if no USB Mass storage devices are installed. Grayed out if the USB Controller is disabled. This setup screen can show a maximum of eight devices on this screen. If more than eight devices are installed in the system, the 'USB Devices Enabled' displays the correct count, but only the first eight devices can display here.
USB 2.0 controller	**Enabled** Disabled	Onboard USB ports are enabled to support USB 2.0 mode. Contact your OS vendor regarding OS support of this feature.	Grayed out if the USB Controller is disabled.

5.3.2.2.6 PCI Screen

The PCI Screen allows the user to configure the PCI add-in cards, onboard NIC controllers, and video options.

To access this screen from the Main screen, select **Advanced** > **PCI**.

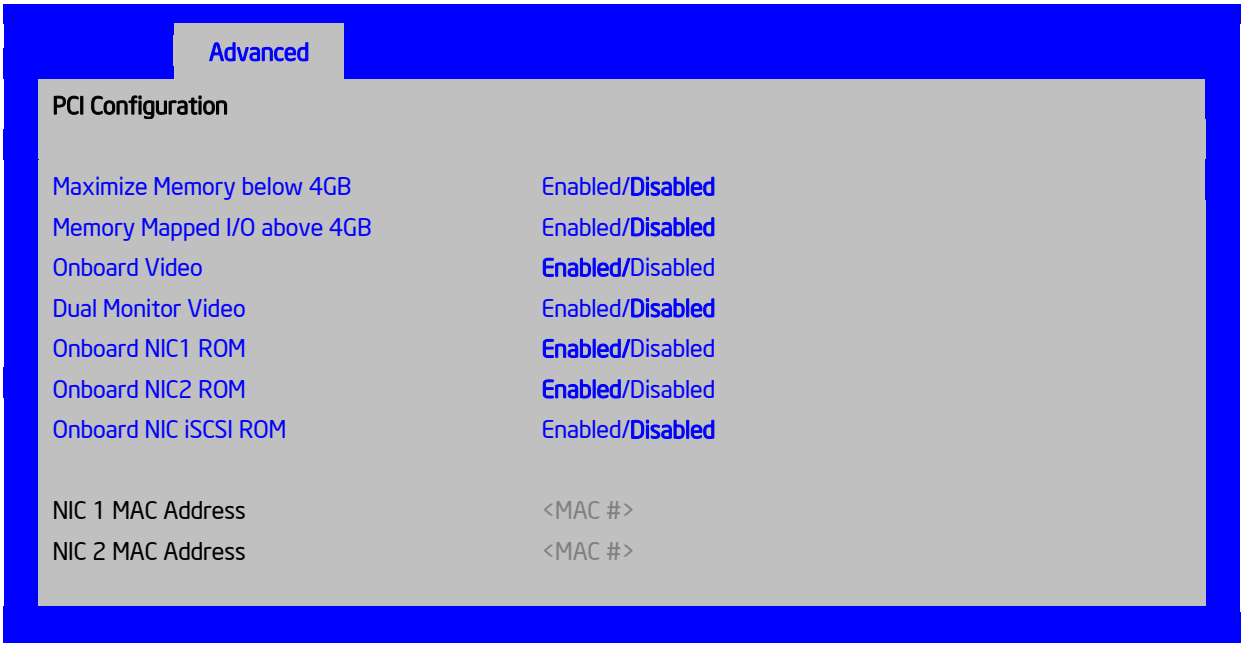


Figure 36. Setup Utility — PCI Configuration Screen Display

Table 29. Setup Utility — PCI Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Maximize Memory below 4GB	Enabled **Disabled**	BIOS maximizes memory usage below 4GB for an OS without PAE support, depending on the system configuration. Only enable for an OS without PAE support	
Memory Mapped I/O above 4GB	Enabled **Disabled**	Enable or disable memory mapped I/O of 64-bit PCI devices to 4 GB or greater address space.	
Onboard Video	**Enabled** Disabled	Onboard video controller. Warning: System video is completely disabled if this option is disabled and an add-in video adapter is not installed.	When disabled, the system requires an add-in video card for the video to be seen.
Dual Monitor Video	Enabled **Disabled**	If enabled. both the onboard video controller and an add-in video adapter are enabled for system video. The onboard video controller becomes the primary video device.	
Onboard NIC1 ROM	**Enabled** Disabled	If enabled. loads the embedded option ROM for the onboard network controllers. Warning: If [Disabled] is selected, NIC1 cannot be used to boot or wake the system.	
Onboard NIC2 ROM	**Enabled** Disabled	If enabled. loads the embedded option ROM for the onboard network controllers. Warning: If [Disabled] is selected, NIC2 cannot be used to boot or wake the system.	

Setup Item	Options	Help Text	Comments
Onboard NIC iSCSI ROM	Enabled **Disabled**	If enabled. loads the embedded option ROM for the onboard network controllers. Warning: If [Disabled] is selected, NIC1 and NIC2 cannot be used to boot or wake the system.	This option is grayed out and not accessible if either the NIC1 or NIC2 ROMs are enabled.
NIC 1 MAC Address	No entry allowed		**Information only.** 12 hex digits of the MAC address.
NIC 2 MAC Address	No entry allowed		**Information only.** 12 hex digits of the MAC address.

5.3.2.2.7 System Acoustic and Performance Configuration

The System Acoustic and Performance Configuration screen allows the user to configure the thermal characteristics of the system.

To access this screen from the Main screen, select **Advanced** > **System Acoustic and Performance Configuration**.

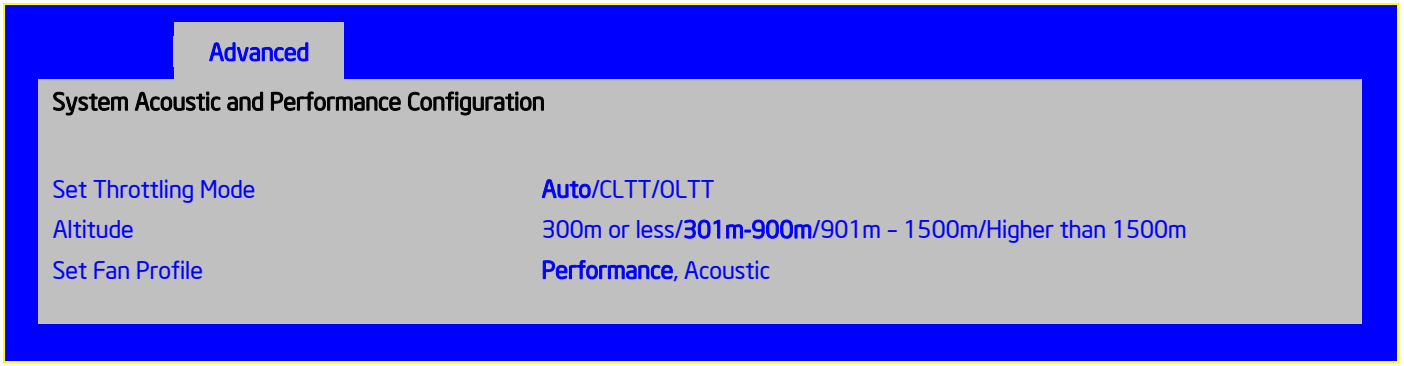


Figure 37. Setup Utility — System Acoustic and Performance Configuration Screen Display

Table 30. Setup Utility — System Acoustic and Performance Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Set Throttling Mode	**Auto** CLTT OLTT	[Auto] – Auto Throttling mode. [CLTT] – Closed Loop Thermal Throttling Mode. [OLTT] – Open Loop Thermal Throttling Mode.	
Altitude	300m or less **301m-900m** 901m-1500m Higher than 1500m	[300m or less] (980ft or less) Optimal performance setting near sea level. [301m - 900m] (980ft - 2950ft) Optimal performance setting at moderate elevation. [901m – 1500m] (2950ft – 4920ft) Optimal performance setting at high elevation. [Higher than 1500m] (4920ft or greater) Optimal performance setting at the highest elevations.	
Set Fan Profile	**Performance** Acoustics	[Performance] - Fan control provides primary system cooling before attempting to throttle memory. [Acoustic] - The system will favor using throttling of memory over boosting fans to cool the system if thermal thresholds are met.	If CLTT is enabled, this option is hidden.

5.3.2.3 Security Screen

The Security screen allows the user to enable and set the user and administrative password. This is done to lock out the front panel buttons so they cannot be used. This screen also allows the user to enable and activate the Trusted Platform Module (TPM) security settings.

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

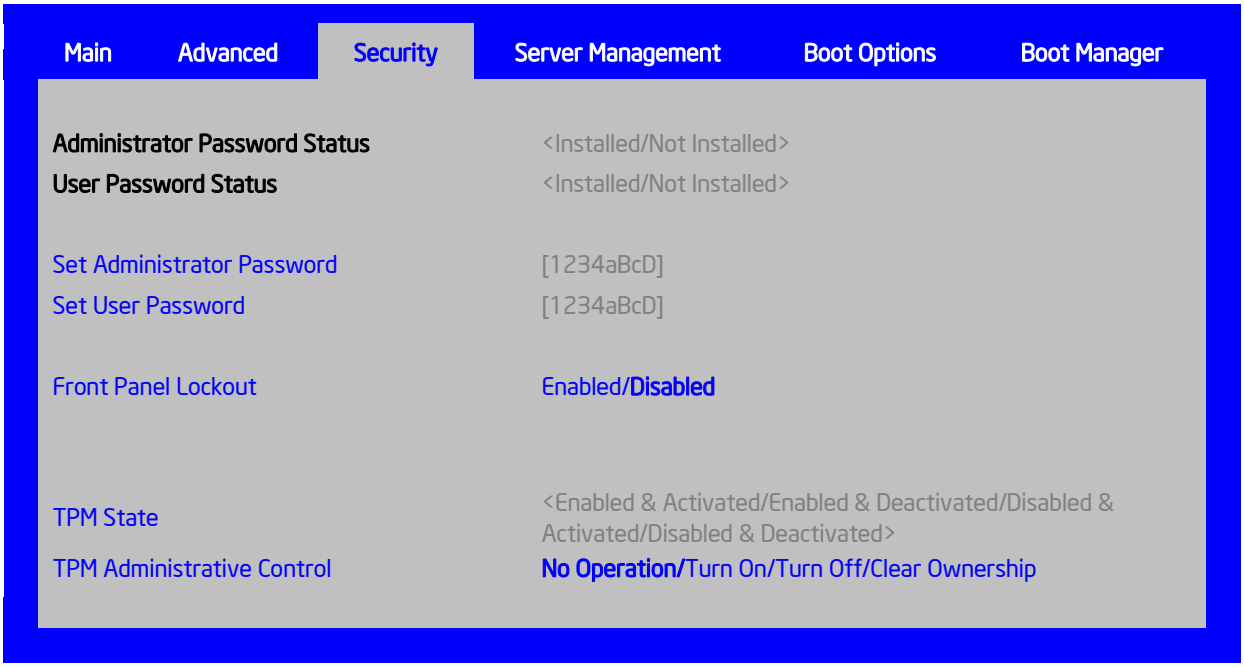


Figure 38. Setup Utility — Security Configuration Screen Display

Table 31. Setup Utility — Security Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Administrator Password Status	<Installed Not Installed>		**Information only.** Indicates the status of the administrator password.
User Password Status	<Installed Not Installed>		**Information only.** Indicates the status of the user password.
Set Administrator Password	[123aBcD]	Administrator password is used to control change access in BIOS Setup Utility. Only alphanumeric characters can be used. Maximum length is 7 characters. It is case sensitive. **Note:** Administrator password must be set in order to use the user account.	This option is only to control access to the setup. Administrator has full access to all the setup items. Clearing the Administrator password also clears the user password.
Set User Password	[123aBcD]	User password is used to control entry access to BIOS Setup Utility. Only alphanumeric characters can be used. Maximum length is 7 characters. It is case sensitive. **Note:** Removing the administrator password also automatically removes the user password.	Available only if the administrator password is installed. This option only protects the setup. User password only has limited access to the setup items.
Front Panel Lockout	Enabled **Disabled**	If enabled, locks the power button and reset button on the system's front panel. If [Enabled] is selected, power and reset must be controlled via a system management interface.	
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 does not execute commands that use the TPM functions and TPM security operations are not available. An enabled and deactivated TPM is in the same state as a disabled TPM except setting of the TPM ownership is allowed if not present already. An enabled and activated TPM executes all commands that use the TPM functions and TPM security operations are also available.

Setup Item	Options	Help Text	Comments
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.	

*Not Available in Intel® Server Boards S5520HC, S5500HCV and S5520HCT, which have no TPM.

** Grayed-out at [No Operation] state in Intel® Server Boards S5520HC, S5500HCV and S5520HCT, which have no TPM.

5.3.2.4 Server Management Screen

The Server Management screen allows the user to configure several server management features. This screen also provides an access point to the screens for configuring console redirection and displaying system information.

To access this screen from the Main screen, select Server Management.

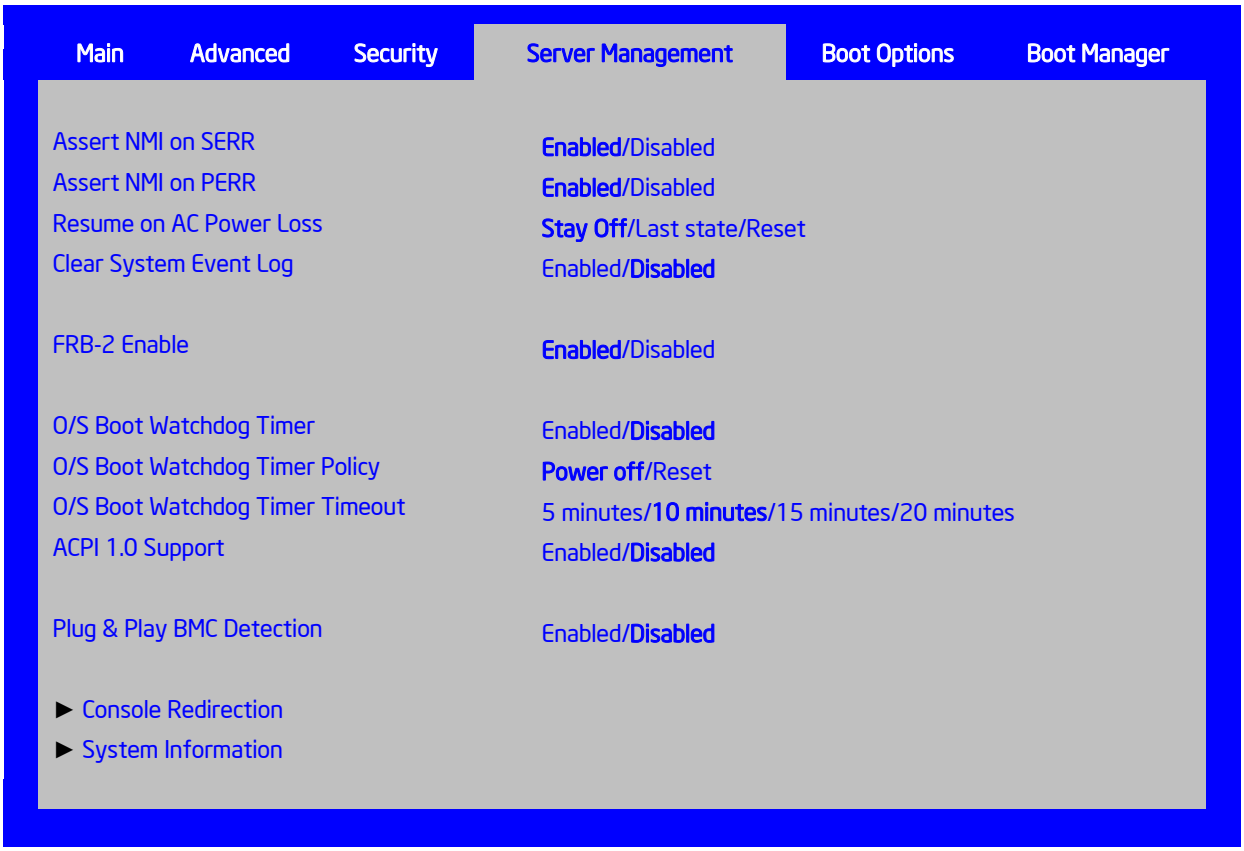


Figure 39. Setup Utility — Server Management Configuration Screen Display

Table 32. Setup Utility — Server Management Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Assert NMI on SERR	**Enabled** Disabled	On SERR, generate an NMI and log an error. **Note**: [Enabled] must be selected for the Assert NMI on PERR setup option to be visible.	
Assert NMI on PERR	**Enabled** Disabled	On PERR, generate an NMI and log an error. **Note**: This option is only active if the Assert NMI on SERR option is [Enabled] selected.	
Resume on AC Power Loss	**Stay Off** Last state Reset	System action to take on AC power loss recovery. [Stay Off] - System stays off. [Last State] - System returns to the same state before the AC power loss. [Reset] - System powers on.	
Clear System Event Log	Enabled **Disabled**	If enabled, clears the System Event Log. All current entries will be lost. **Note**: This option is reset to [Disabled] after a reboot.	
FRB-2 Enable	**Enabled** Disabled	Fault Resilient Boot (FRB). If enabled, the BIOS programs the BMC watchdog timer for approximately 6 minutes. If the BIOS does not complete POST before the timer expires, the BMC resets the system.	

Setup Item	Options	Help Text	Comments
O/S Boot Watchdog Timer	Enabled **Disabled**	If enabled, the BIOS programs the watchdog timer with the timeout value selected. If the OS does not complete booting before the timer expires, the BMC resets the system and an error is logged. Requires OS support or Intel Management Software.	
O/S Boot Watchdog Timer Policy	**Power Off** Reset	If the OS boot watchdog timer is enabled, this is the system action taken if the watchdog timer expires. [Reset] - System performs a reset. [Power Off] - System powers off.	Grayed out when O/S Boot Watchdog Timer is disabled.
O/S Boot Watchdog Timer Timeout	5 minutes **10 minutes** 15 minutes 20 minutes	If the OS watchdog timer is enabled, this is the timeout value used by the BIOS to configure the watchdog timer.	Grayed out when O/S Boot Watchdog Timer is disabled.
Plug & Play BMC Detection	Enabled **Disabled**	If enabled, the BMC is detectable by OSs that support plug and play loading of an IPMI driver. Do not enable if your OS does not support this driver.	
ACPI 1.0 Support	Enabled **Disabled**	[Enabled] - Publish ACPI 1.0 version of FADT in Root System Description Table. May be required for compatibility with OS versions that only support ACPI 1.0.	Needs to be [Enabled] for Microsoft Windows 2000* support.
Console Redirection		View/Configure console redirection information and settings.	Takes the user to the Console Redirection screen.
System Information		View system information	Takes the user to the System Information screen.

5.3.2.4.1 Console Redirection Screen

The Console Redirection screen allows the user to enable or disable console redirection and configure the connection options for this feature.

To access this screen from the Main screen, select **Server Management** > **Console Redirection**.

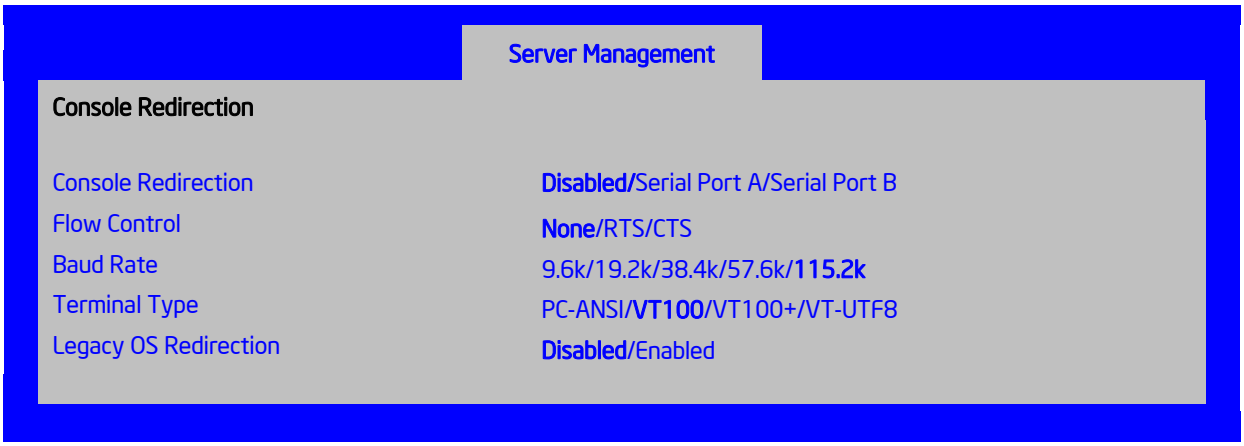


Figure 40. Setup Utility — Console Redirection Screen Display

Table 33. Setup Utility — Console Redirection Configuration Fields

Setup Item	Options	Help Text
Console Redirection	**Disabled** Serial Port A Serial Port B	Console redirection allows a serial port to be used for server management tasks. [Disabled] - No console redirection. [Serial Port A] - Configure serial port A for console redirection. [Serial Port B] - Configure serial port B for console redirection. Enabling this option disables the display of the Quiet Boot logo screen during POST.
Flow Control	**None** RTS/CTS	Flow control is the handshake protocol. Setting must match the remote terminal application. [None] - Configure for no flow control. [RTS/CTS] - Configure for hardware flow control.
Baud Rate	9600 19.2K 38.4K 57.6K **115.2K**	Serial port transmission speed. Setting must match the remote terminal application.
Terminal Type	PC-ANSI **VT100** VT100+ VT-UTF8	Character formatting used for console redirection. Setting must match the remote terminal application.
Legacy OS Redirection	**Disabled** Enabled	This option enables legacy OS redirection (i.e., DOS) on serial port. If it is enabled, the associated serial port is hidden from the legacy OS.

5.3.2.5 Server Management System Information Screen

The Server Management System Information screen allows the user to view part numbers, serial numbers, and firmware revisions.

To access this screen from the Main screen, select **Server Management** > **System Information**.

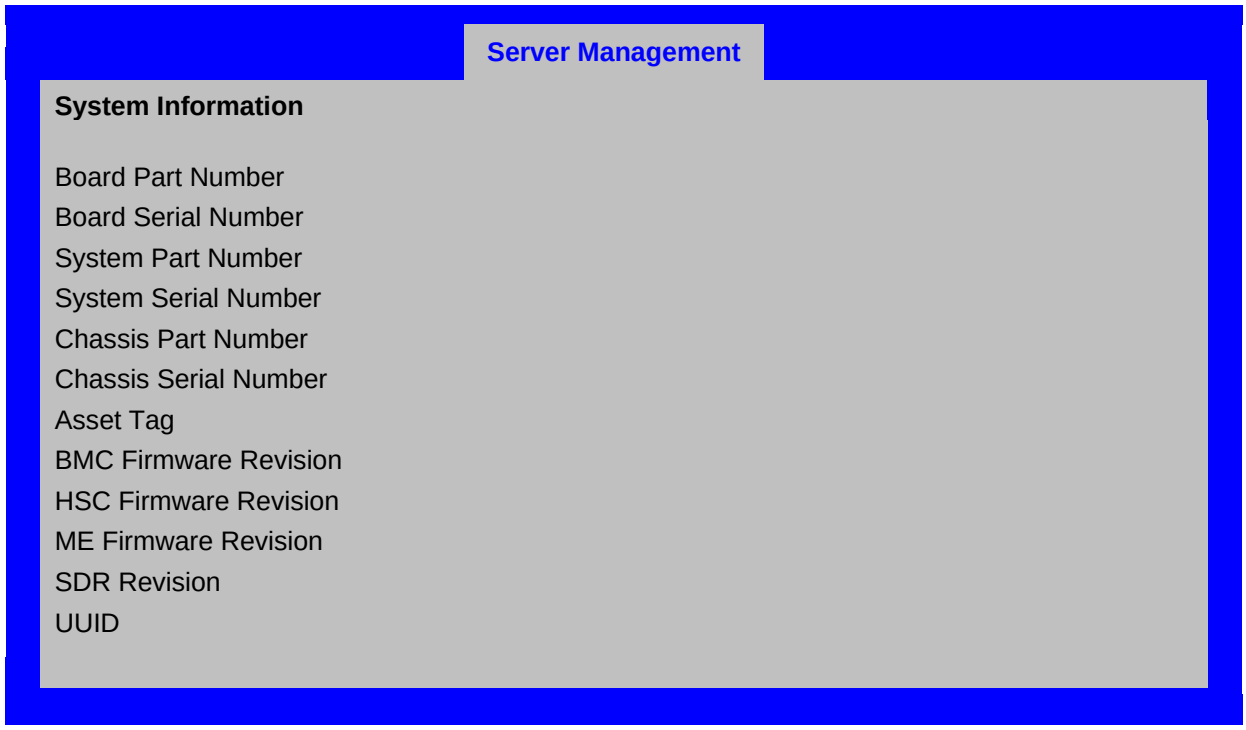


Figure 41. Setup Utility — Server Management System Information Screen Display

Table 34. Setup Utility — Server Management System Information Fields

Setup Item	Comments
Board Part Number	**Information only**
Board Serial Number	**Information only**
System Part Number	**Information only**
System Serial Number	**Information only**
Chassis Part Number	**Information only**
Chassis Serial Number	**Information only**
Asset Tag	**Information only**
BMC Firmware Revision	**Information only**
HSC Firmware Revision	**Information only** If there is no HSC installed, the Firmware Revision Number will appear as “0.00”.
ME Firmware Revision	**Information only**
SDR Revision	**Information only**
UUID	**Information only**

5.3.2.6 Boot Options Screen

The Boot Options screen displays any bootable media encountered during POST and allows the user to configure the desired boot device.

To access this screen from the Main screen, select Boot Options.

Figure 42. Setup Utility — Boot Options Screen Display

Table 35. Setup Utility — Boot Options Screen Fields

Setup Item	Options	Help Text	Comments
Boot Timeout	0 - 65535	The number of seconds the BIOS should pause at the end of POST to allow the user to press the [F2] key for entering the BIOS Setup utility. Valid values are 0-65535. Zero is the default. A value of 65535 causes the system to go to the Boot Manager menu and wait for user input for every system boot.	After entering the necessary timeout, press the Enter key to register that timeout value to the system. These settings are in seconds.
Boot Option #x	Available boot devices.	Set system boot order by selecting the boot option for this position.	
Hard Disk Order		Set the order of the legacy devices in this group.	Displays when one or more hard disk drives are in the system.
CDROM Order		Set the order of the legacy devices in this group.	Displays when one or more CD-ROM drives are in the system.
Floppy Order		Set the order of the legacy devices in this group.	Displays when one or more floppy drives are in the system.
Network Device Order		Set the order of the legacy devices in this group.	Displays when one or more of these devices are available in the system.
BEV Device Order		Set the order of the legacy devices in this group.	Displays when one or more of these devices are available in the system.
Add New Boot Option		Add a new EFI boot option to the boot order.	This option is only displayed if an EFI bootable device is available to the system (for example, a USB drive).
Delete Boot Option		Remove an EFI boot option from the boot order.	If the EFI shell is deleted, it is restored on the next system reboot. It cannot be permanently deleted.
EFI Optimized Boot	Enabled **Disabled**	If enabled, the BIOS only loads modules required for booting EFI-aware Operating Systems.	Grayed out when [SW RAID] SATA Mode is Enabled. SW RAID can only be used in Legacy Boot mode.
Use Legacy Video for EFI OS	Enabled **Disabled**	If enabled, the BIOS will use the legacy video ROM instead of the EFI video ROM.	Only displays when EFI Optimized Boot is enabled.
Boot Option Retry	Enabled **Disabled**	If enabled, this continually retries non-EFI-based boot options without waiting for user input.	
USB Boot Priority	**Enabled** Disabled	If enabled newly discovered USB devices will be put to the top of their boot device category. If disabled newly discovered USB devices will be put at the bottom of the respective list	

If all types of bootable devices are installed in the system, then the default boot order is:

1. CD/DVD-ROM
2. Floppy Disk Drive
3. Hard Disk Drive
4. PXE Network Device
5. BEV (Boot Entry Vector) Device
6. EFI Shell and EFI Boot paths

5.3.2.6.1 Add New Boot Option Screen

The Add Boot Option screen allows the user to remove an EFI boot option from the boot order.

To access this screen from the Main screen, select **Boot Options** > **Delete Boot Options**.

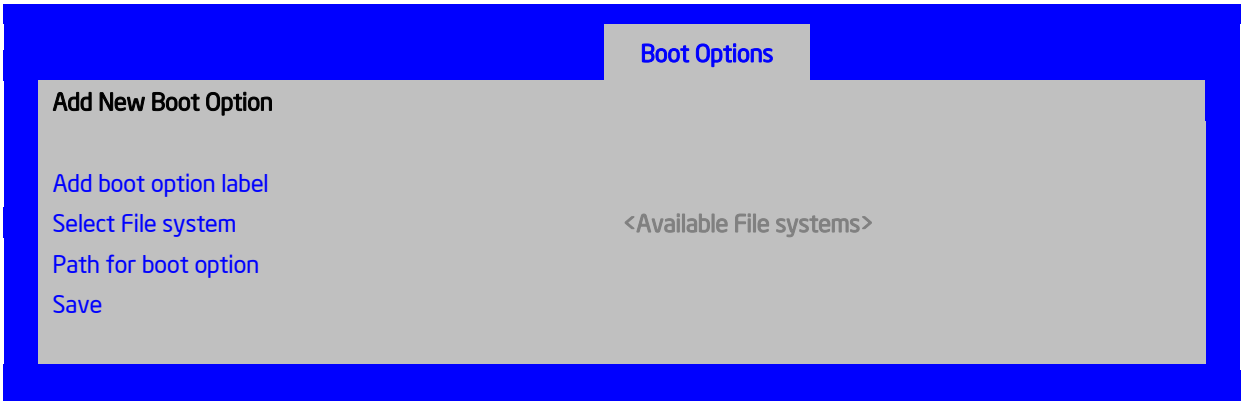


Figure 43. Setup Utility — Add New Boot Option Screen Display

Table 36. Setup Utility — Add New Boot Option Fields

Setup Item	Options	Help Text
Add boot option label		Create the label for the new boot option.
Select File system	Select one from list provided.	Select one file system from the list.
Path for boot option		Enter the path to boot option in the format \path\filename.efi
Save		Save the boot option.

5.3.2.6.2 Delete Boot Option Screen

The Delete Boot Option screen allows the user to remove an EFI boot option from the boot order. Note that while you can delete the Internal EFI Shell in this screen, it is restored to the Boot Order on the next reboot. You cannot permanently delete the Internal EFI Shell.

To access this screen from the Main screen, select **Boot Options** > **Delete Boot Options**.

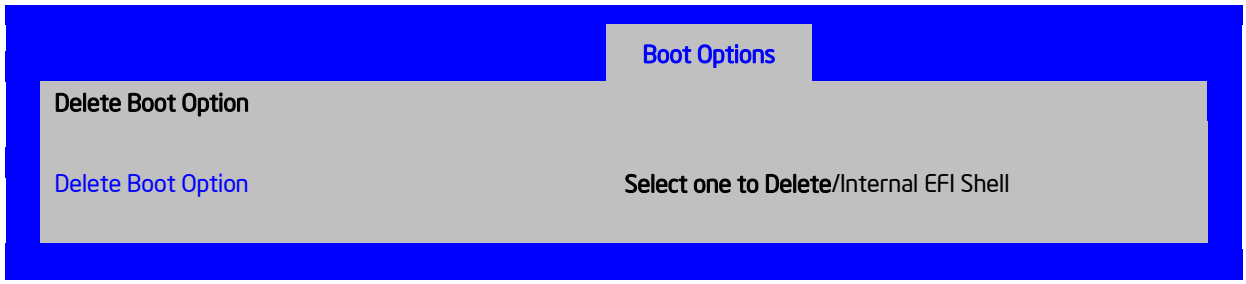


Figure 44. Setup Utility — Delete Boot Option Screen Display

Table 37. Setup Utility — Delete Boot Option Fields

Setup Item	Options	Help Text	Comments
Delete Boot Option	Select one to Delete Internal EFI Shell	Remove an EFI boot option from the boot order.	If the EFI shell is deleted, it is restored on the next system reboot. It cannot be permanently deleted.

5.3.2.6.3 Hard Disk Order Screen

The Hard Disk Order screen allows the user to control the hard disks.

To access this screen from the Main screen, select **Boot Options** > **Hard Disk Order**.

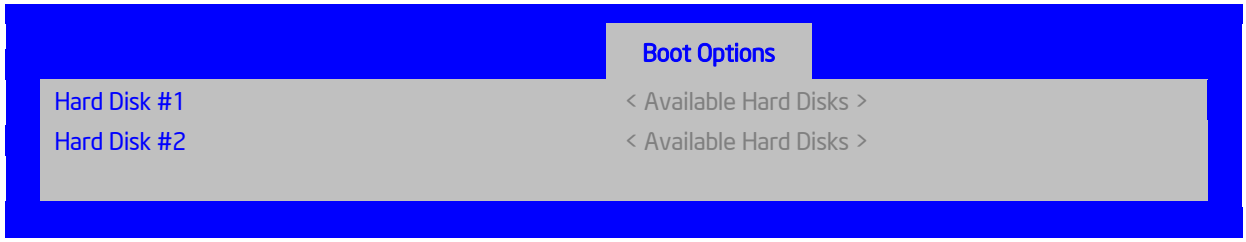


Figure 45. Setup Utility — Hard Disk Order Screen Display

Table 38. Setup Utility — Hard Disk Order Fields

Setup Item	Options	Help Text
Hard Disk #1	Available Legacy devices for this Device group.	Set system boot order by selecting the boot option for this position.
Hard Disk #2	Available Legacy devices for this Device group.	Set system boot order by selecting the boot option for this position.

5.3.2.6.4 CDROM Order Screen

The CDROM Order screen allows the user to control the CDROM devices.

To access this screen from the Main screen, select **Boot Options** > **CDROM Order**.

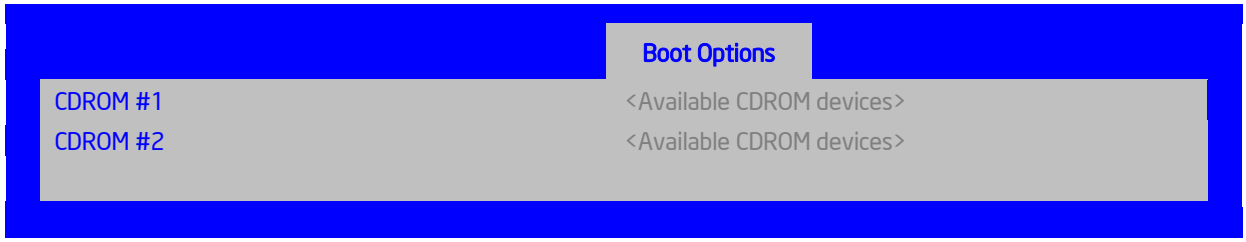


Figure 46. Setup Utility — CDROM Order Screen Display

Table 39. Setup Utility — CDROM Order Fields

Setup Item	Options	Help Text
CDROM #1	Available Legacy devices for this Device group.	Set system boot order by selecting the boot option for this position.
CDROM #2	Available Legacy devices for this Device group.	Set system boot order by selecting the boot option for this position.

5.3.2.6.5 Floppy Order Screen

The Floppy Order screen allows the user to control the floppy drives.

To access this screen from the Main screen, select **Boot Options** > **Floppy Order**.

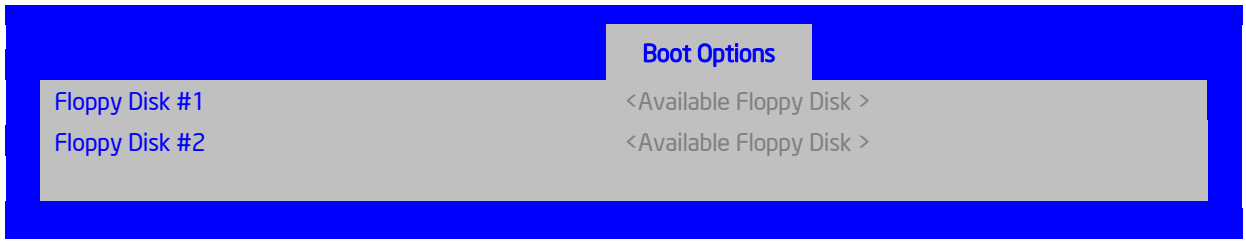


Figure 47. Setup Utility — Floppy Order Screen Display

Table 40. Setup Utility — Floppy Order Fields

Setup Item	Options	Help Text
Floppy Disk #1	Available Legacy devices for this Device group.	Set system boot order by selecting the boot option for this position.

Setup Item	Options	Help Text
Floppy Disk #2	Available Legacy devices for this Device group.	Set system boot order by selecting the boot option for this position.

5.3.2.6.6 Network Device Order Screen

The Network Device Order screen allows the user to control the network bootable devices.

To access this screen from the Main screen, select **Boot Options** > **Network Device Order**.

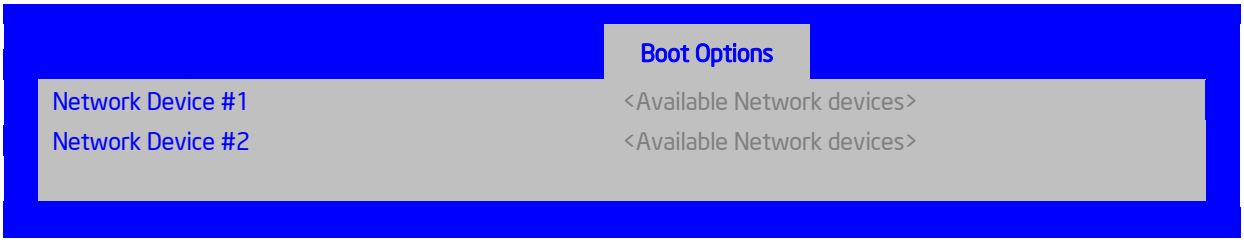


Figure 48. Setup Utility — Network Device Order Screen Display

Table 41. Setup Utility — Network Device Order Fields

Setup Item	Options	Help Text
Network Device #1	Available Legacy devices for this Device group.	Set system boot order by selecting the boot option for this position.
Network Device #2	Available Legacy devices for this Device group.	Set system boot order by selecting the boot option for this position.

5.3.2.6.7 BEV Device Order Screen

The BEV Device Order screen allows the user to control the BEV bootable devices.

To access this screen from the Main screen, select **Boot Options** > **BEV Device Order**.

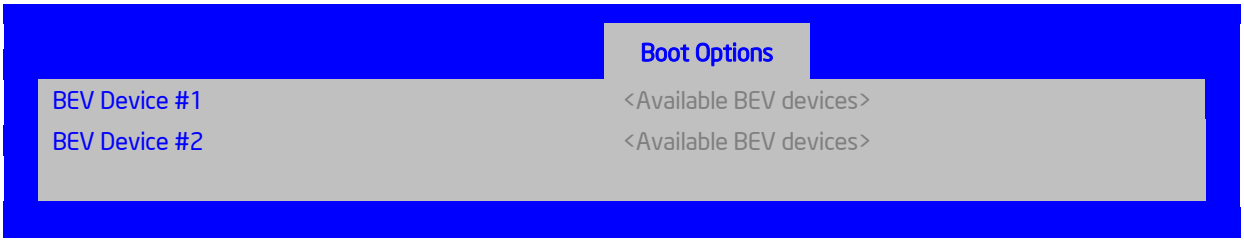


Figure 49. Setup Utility — BEV Device Order Screen Display

Table 42. Setup Utility — BEV Device Order Fields

Setup Item	Options	Help Text
BEV Device #1	Available Legacy devices for this Device group.	Set system boot order by selecting the boot option for this position.
BEV Device #2	Available Legacy devices for this Device group.	Set system boot order by selecting the boot option for this position.

5.3.2.7 Boot Manager Screen

The Boot Manager screen allows the user to view a list of devices available for booting, and to select a boot device for immediately booting the system.

To access this screen from the Main screen, select Boot Manager.

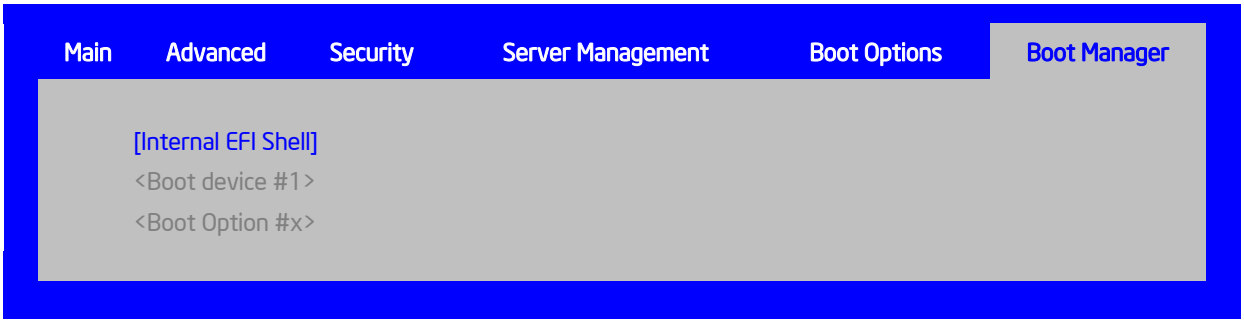


Figure 50. Setup Utility — Boot Manager Screen Display

Table 43. Setup Utility — Boot Manager Screen Fields

Setup Item	Help Text
Internal EFI Shell	Select this option to boot now. **Note**: This list is not the system boot option order. Use the Boot Options menu to view and configure the system boot option order.
Boot Device #x	Select this option to boot now. **Note**: This list is not the system boot option order. Use the Boot Options menu to view and configure the system boot option order.

5.3.2.8 Error Manager Screen

The Error Manager screen displays any errors encountered during POST.

Figure 51. Setup Utility — Error Manager Screen Display

Table 44. Setup Utility — Error Manager Screen Fields

Setup Item	Comments
Displays System Errors	**Information only.** Displays errors that occurred during POST.

5.3.2.9 Exit Screen

The Exit screen allows the user to choose whether to save or discard the configuration changes made on the other screens. It also allows the user to restore the server to the factory defaults or to save or restore them to the set of user-defined default values. If Load Default Values is selected, the factory default settings (noted in bold in the tables in this chapter) are applied. If Load User Default Values is selected, the system is restored to previously-saved, user-defined default values.

Figure 52. Setup Utility — Exit Screen Display

Table 45. Setup Utility — Exit Screen Fields

Setup Item	Help Text	Comments
Save Changes and Exit	Exit the BIOS Setup utility after saving changes. The system reboots if required. The [F10] key can also be used.	User prompted for confirmation only if any of the setup fields were modified.
Discard Changes and Exit	Exit the BIOS Setup utility without saving changes. The [Esc] key can also be used.	User prompted for confirmation only if any of the setup fields were modified.
Save Changes	Save changes without exiting the BIOS Setup Utility. **Note**: Saved changes may require a system reboot before taking effect.	User prompted for confirmation only if any of the setup fields were modified.
Discard Changes	Discard changes made since the last Save Changes operation was performed.	User prompted for confirmation only if any of the setup fields were modified.
Load Default Values	Load factory default values for all BIOS Setup utility options. The [F9] key can also be used.	User prompted for confirmation.
Save as User Default Values	Save current BIOS Setup utility values as custom user default values. If needed, the user default values can be restored via the Load User Default Values option below. **Note**: Clearing the CMOS or NVRAM does not cause the User Default values to be reset to the factory default values.	User prompted for confirmation.
Load User Default Values	Load user default values.	User prompted for confirmation.

6. Connector/Header Locations and Pin-outs

6.1 Board Connector Information

The following section provides detailed information regarding all connectors, headers, and jumpers on the server boards.

The following table lists all connector types available on the board and the corresponding preference designators printed on the silkscreen.

Table 46. Board Connector Matrix

Connector	Quantity	Reference Designators	Connector Type	Pin Count
Power supply	4	J1K3 J9A1 J9K1 J9K2	Main power CPU 1 power CPU 2 Power P/S aux/IPMB	24 8 8 5
CPU	2	U7J1, U7C1	CPU sockets	1366
Main memory	12	J4F1, J5F1*, J5F2, J5F3*, J6F1, J6F2*, J8F1, J8F2, J8F3, J9F1, J9F2, J9F3	DIMM sockets	240
PCI Express* x8	4	J2B1, J2B2, J3B1, J4B1*	Card edge	
PCI Express* x16	1	J4B2	Card edge	
32-bit PCI	1	J1B2,	Card edge	
Intel® RMM3	1	J1C1	Mezzanine	34
SAS Module Slot	1	J2J1	Mezzanine	50
SATA Software RAID 5 Key	1	J1F2	Key holder	3
System fans	4	J1K1, J1K2, J1K4, J1K5	Header	6
System fans	1	J9A2	Header	4
CPU fans	2	J7K1, J9A3	Header	4
Battery	1	BT5B1	Battery holder	3
Stacked RJ45/2xUSB	2	J5A1, J6A1	External LAN built-in magnetic and dual USB	22
Video	1	J7A1	External DSub	15
Serial port A	1	J8A1	External DB9	9
Serial port B	1	J1B1	Header	9
Front panel	1	J1B3	Header	24
Internal USB	2	J1D1, J1D2	Header	10
USB Solid State Drive	1	J2D2	Low profile header	10
Internal USB	1	J1H2	Header	4
Chassis Intrusion	1	J1F6	Header	2
Serial ATA	6	J1G1, J1G4, J1G5, J1E3, J1F1, J1F4	Header	7
HSBP	2	J1F5, J1G3	Header	4
SATA SGPIO	1	J1G2	Header	4
LCP/IPMB	1	J1G6	Header	4

Connector	Quantity	Reference Designators	Connector Type	Pin Count
Configuration jumpers	4	J1E6 (CMOS Clear), J1E2 (ME Force Update), J1E4 (Password Clear), J1E5 (BIOS Recovery), J1H1 (BMC Force Update),	Jumper	3
HDD Led	1	J1E1	Header	2

* Empty on Intel® Server Board S5500HCV.

6.2 Power Connectors

The main power supply connection uses an SSI-compliant 2x12 pin connector (J1K3).

Three additional power-related connectors also exist:

- Two SSI-compliant 2x4 pin power connectors (J9A1, J9K1) to provide 12-V power to the CPU voltage regulators and memory.
- One SSI-compliant 1x5 pin connector (J9K2) to provide I^2C monitoring of the power supply.

The following tables define these connector pin-outs.

Table 47. Main Power Connector Pin-out (J1K3)

Pin	Signal	Color	Pin	Signal	Color
1	+3.3 Vdc	Orange	13	+3.3 Vdc	Orange
2	+3.3 Vdc	Orange	14	-12 Vdc	Blue
3	GND	Black	15	GND	Black
4	+5 Vdc	Red	16	PS_ON#	Green
5	GND	Black	17	GND	Black
6	+5 Vdc	Red	18	GND	Black
7	GND	Black	19	GND	Black
8	PWR_OK	Gray	20	RSVD_(-5 V)	White
9	5 VSB	Purple	21	+5 Vdc	Red
10	+12 Vdc	Yellow	22	+5 Vdc	Red
11	+12 Vdc	Yellow	23	+5 Vdc	Red
12	+3.3 Vdc	Orange	24	GND	Black

Table 48. CPU 1 Power Connector Pin-out (J9A1)

Pin	Signal	Color
1	GND of Pin 5	Black
2	GND of Pin 6	Black
3	GND of Pin 7	Black
4	GND of Pin 8	Black
5	+12 Vdc CPU1	Yellow/black
6	+12 Vdc CPU1	Yellow/black
7	+12 Vdc DDR3_CPU1	Yellow/black
8	+12 Vdc DDR3_CPU1	Yellow/black

Table 49. CPU 2 Power Connector Pin-out (J9K1)

Pin	Signal	Color
1	GND of Pin 5	Black
2	GND of Pin 6	Black
3	GND of Pin 7	Black
4	GND of Pin 8	Black
5	+12 Vdc CPU2	Yellow/black
6	+12 Vdc CPU2	Yellow/black
7	+12 Vdc DDR3_CPU2	Yellow/black
8	+12 Vdc DDR3_CPU2	Yellow/black

Table 50. Power Supply Auxiliary Signal Connector Pin-out (J9K2)

Pin	Signal	Color
1	SMB_CLK_FP_PWR_R	Orange
2	SMB_DAT_FP_PWR_R	Black
3	SMB_ALRT_3_ESB_R	Red
4	3.3 V SENSE-	Yellow
5	3.3 V SENSE+	Green

6.3 System Management Headers

6.3.1 Intel® Remote Management Module 3 Connector

A 34-pin Intel® RMM3 connector (J1C1) is included on the server boards to support the optional Intel® Remote Management Module 3. These server boards do not support third-party management cards.

Note: This connector is not compatible with the Intel® Remote Management Module (Intel® RMM) or the Intel® Remote Management Module 2 (Intel® RMM2).

Table 51. Intel® RMM3 Connector Pin-out (J1C1)

Pin	Signal Name	Pin	Signal Name
1	3V3_AUX	2	RMII_MDIO
3	3V3_AUX	4	RMII_MDC
5	GND	6	RMII_RXD1
7	GND	8	RMII_RXD0
9	GND	10	RMII_RX_DV
11	GND	12	RMII_REF_CLK
13	GND	14	RMII_RX_ER
15	GND	16	RMII_TX_EN
17	GND	18	KEY (pin removed)
19	GND	20	RMII_TXD0
21	GND	22	RMII_TXD1
23	3V3_AUX	24	SPI_CS_N
25	3V3_AUX	26	NC (spare)

Pin	Signal Name	Pin	Signal Name
27	3V3_AUX	28	SPI_DO
29	GND	30	SPI_CLK
31	GND	32	SPI_DI
33	GND	34	RMM3_Present_N (pulled high on baseboard and shorted to ground on the plug-in module)

6.3.2 LCP/IPMB Header

Table 52. LCP/IPMB Header Pin-out (J1G6)

Pin	Signal Name	Description
1	SMB_IPMB_5VSB_DAT	BMC IMB 5 V standby data line
2	GND	Ground
3	SMB_IPMB_5VSB_CLK	BMC IMB 5 V standby clock line
4	P5V_STBY	+5 V standby power

6.3.3 HSBP Header

Table 53. HSBP Header Pin-out (J1F5, J1G3)

Pin	Signal Name	Description
1	SMB_IPMB_5V_DAT	BMC IMB 5 V Data Line
2	GND	Ground
3	SMB_IPMB_5V_CLK	BMC IMB 5V Clock Line
4	P5V – HSBP_A GND – HSBP_B	+5 V for HSBP A Ground for HSBP B

6.3.4 SGPIO Header

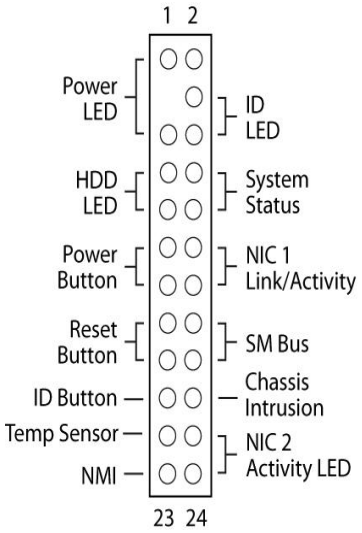
Table 54. SGPIO Header Pin-out (J1G2)

Pin	Signal Name	Description
1	SGPIO_CLOCK	SGPIO Clock Signal
2	SGPIO_LOAD	SGPIO Load Signal
3	SGPIO_DATAOUT0	SGPIO Data Out
4	SGPIO_DATAOUT1	SGPIO Data In

6.4 Front Panel Connector

The server boards provide a 24-pin SSI front panel connector (J1B3) for use with Intel® and third-party chassis. The following table provides the pin-out for this connector:

Table 55. Front Panel SSI Standard 24-pin Connector Pin-out (J1B3)



Pin	Signal Name	Description	Pin	Signal Name	Description
1	P3V3_STBY (Power_LED_Anode)	Power LED +	2	P3V3_STBY	Front Panel Power
3	Key	No Connection	4	P5V_STBY (ID LED Anode)	ID LED +
5	FP_PWR_LED_N	Power LED -	6	FP_ID_LED_BUF_N	ID LED -
7	P3V3 (HDD_ACTIVITY_Anode)	HDD Activity LED +	8	FP_LED_STATUS_GREEN_N	Status LED Green -
9	LED_HDD_ACTIVITY_N	HDD Activity LED -	10	FP_LED_STATUS_AMBER_N	Status LED Amber -
11	FP_PWR_BTN_N	Power Button	12	NIC1_ACT_LED_N	NIC 1 Activity LED -
13	GND (Power Button GND)	Power Button Ground	14	NIC1_LINK_LED_N	NIC 1 Link LED -
15	BMC_RST_BTN_N	Reset Button	16	SMB_SENSOR_3V3STB_DATA	SMB Sensor DATA
17	BND (Reset GND)	Reset Button Ground	18	SMB_SENSOR_3V3STB_CLK	SMB Sensor Clock
19	FP_ID_BTN_N	ID Button	20	FP_CHASSIS_INTRU	Chassis Intrusion
21	FM_SIO_TEMP_SENSOR	Front Panel Temperature Sensor	22	NIC2_ACT_LED_N	NIC 2 Activity LED -
23	FP_NMI_BTN_N	NMI Button	24	NIC2_LINK_LED_N	NIC 2 Link LED -

6.5 I/O Connectors

6.5.1 VGA Connector

The following table details the pin-out definition of the VGA connector (J7A1) that is part of the stacked video/serial port A connector.

Table 56. VGA Connector Pin-out (J7A1)

Pin	Signal Name	Description
1	V_IO_R_CONN	Red (analog color signal R)
2	V_IO_G_CONN	Green (analog color signal G)
3	V_IO_B_CONN	Blue (analog color signal B)
4	TP_VID_CONN_B4	No connection
5	GND	Ground
6	GND	Ground
7	GND	Ground
8	GND	Ground
9	TP_VID_CONN_B9	No connection
10	GND	Ground
11	TP_VID_CONN_B11	No connection
12	V_IO_DDCDAT	DDCDAT
13	V_IO_HSYNC_CONN	HSYNC (horizontal sync)
14	V_IO_VSYNC_CONN	VSYNC (vertical sync)
15	V_IO_DDCCLK	DDCCLK

6.5.2 NIC Connectors

The server boards provide two stacked RJ-45/2xUSB connectors side-by-side on the back edge of the board (J5A1, J6A1). The pin-out for NIC connectors is identical and defined in the following table.

Table 57. RJ-45 10/100/1000 NIC Connector Pin-out (J5A1, J6A1)

Pin	Signal Name
1	GND
2	P1V8_NIC
3	NIC_A_MDI3P
4	NIC_A_MDI3N
5	NIC_A_MDI2P
6	NIC_A_MDI2N
7	NIC_A_MDI1P
8	NIC_A_MDI1N
9	NIC_A_MDI0P
10	NIC_A_MDI0N
11	NIC_LINKA_1000_N (LED
12	NIC_LINKA_100_N (LED)
13	NIC_ACT_LED_N
14	NIC_LINK_LED_N
15	GND
16	GND

6.5.3 SATA Connectors

The server boards provide up to six SATA connectors: SATA-0 (J1G5), SATA-1 (J1G4), SATA-2 (J1G1), SATA-3 (J1F4), SATA-4 (J1F1), and SATA-5 (J1E3).

The pin configuration for each connector is identical and defined in the following table:

Table 58. SATA/SAS Connector Pin-out (J1E3, J1G1, J1G4, J1G5, J1F1, J1F4)

Pin	Signal Name	Description
1	GND	Ground
2	SATA TX_P_C	Positive side of transmit differential pair
3	SATA TX_N_C	Negative side of transmit differential pair
4	GND	Ground
5	SATA _RX_N_C	Negative side of receive differential pair
6	SATA _RX_P_C	Positive side of receive differential pair
7	GND	Ground

6.5.4 SAS Module Slot

The server boards provide one SAS module slot (J2J1) to support the Intel® SAS Entry RAID Module AXX4SASMOD card. The following table defines the pin-out:

Table 59. SAS Module Slot Pin-out (J2J1)

Pin	Name	Pin	Name
1	P3V3_AUX	2	RST_LPC_SAS_N
3	SW_RAID_MODE	4	GND
5	PE_ICH10_SAS_SW_C_TP0	6	PE_ICH10_SAS_SW_C_TN0
7	GND	8	GND

Pin	Name	Pin	Name
9	PE_ICH10_SAS_SW_C_TP1	10	PE_ICH10_SAS_SW_C_TN1
11	GND	12	GND
13	PE_ICH10_SAS_SW_C_TN2	14	PE_ICH10_SAS_SW_C_TN2
15	GND	16	GND
17	PE_ICH10_SAS_SW_C_TN3	18	PE_ICH10_SAS_SW_C_TN3
19	GND	20	FM_SAS_PRSNT_N
21	PE_WAKE_N	22	FM_SAS_RST_N
23	P3V3	24	PE_RXN<2>
25	P3V3	26	P3V3_AUX
27	GND	28	PE_ICH10_SAS_SW_RXP0
29	PE_ICH10_SAS_SW_RXN0	30	GND
31	GND	32	PE_ICH10_SAS_SW_RXP1
33	PE_ICH10_SAS_SW_RXN1	34	GND
35	GND	36	PE_ICH10_SAS_SW_RXP2
37	PE_ICH10_SAS_SW_RXN2	38	GND
39	GND	40	PE_ICH10_SAS_SW_RXP3
41	PE_ICH10_SAS_SW_RXN3	42	GND
43	GND	44	CLK_100M_SAS_DP
45	CLK_100M_SAS_DN	46	GND
47	GND	48	P3V3
49	P3V3	50	P3V3

6.5.5 Serial Port Connectors

The server boards provide one external DB9 Serial A port (J8A1) and one internal 9-pin Serial B header (J1B1). The following tables define the pin-outs.

Table 60. External DB9 Serial A Port Pin-out (J8A1)

Pin	Signal Name	Description
1	SPA_DCD	DCD (carrier detect)
2	SPA_SIN_L	RXD (receive data)
3	SPA_SOUT_N	TXD (Transmit data)
4	SPA_DTR	DTR (Data terminal ready)
5	GND	Ground
6	SPA_DSR	DSR (data set ready)
7	SPA_RTS	RTS (request to send)
8	SPA_CTS	CTS (clear to send)
9	SPA_RI	RI (Ring Indicate)

Table 61. Internal 9-pin Serial B Header Pin-out (J1B1)

Pin	Signal Name	Description
1	SPB_DCD	DCD (carrier detect)
2	SPB_DSR	DSR (data set ready)
3	SPB_SIN_L	RXD (receive data)
4	SPB_RTS	RTS (request to send)
5	SPB_SOUT_N	TXD (Transmit data)
6	SPB_CTS	CTS (clear to send)
7	SPB_DTR	DTR (Data terminal ready)
8	SPB_RI	RI (Ring indicate)
9	SPB_EN_N	Enable

6.5.6 USB Connector

The following table details the pin-out of the external USB connectors (J5A1, J6A1) found on the back edge of the server boards.

Table 62. External USB Connector Pin-out (J5A1, J6A1)

Pin	Signal Name	Description
1	USB_OC_5VSB	USB_PWR
2	USB_PN	DATAL0 (Differential data line paired with DATAH0)
3	USB_PP	DATAH0 (Differential data line paired with DATAL0)
4	GND	Ground

Two 2x5 connectors on the server boards (J1D1, J1D2) provide support for four additional USB ports. J1D2 is recommended for front panel USB ports.

Table 63. Internal USB Connector Pin-out (J1D1)

Pin	Signal Name	Description
1	USB_PWR45_5V	USB power (port 4)
2	USB_PWR45_5V	USB power (port 5)
3	USB_ICH_P4N_CONN	USB port 4 negative signal
4	USB_ICH_P5N_CONN	USB port 5 negative signal
5	USB_ICH_P4P_CONN	USB port 4 positive signal
6	USB_ICH_P5P_CONN	USB port 5 positive signal
7	Ground	
8	Ground	
9	Key	No pin
10	TP_USB_ICH_NC	Test point

Table 64. Internal USB Connector Pin-out (J1D2)

Pin	Signal Name	Description
1	USB_PWR68_5VSB	USB power (port 6)
2	USB_PWR68_5VSB	USB power (port 8)
3	USB_ICH_P6N_CONN	USB port 6 negative signal
4	USB_ICH_P8N_CONN	USB port 8 negative signal
5	USB_ICH_P6P_CONN	USB port 6 positive signal
6	USB_ICH_P8P_CONN	USB port 8 positive signal
7	Ground	
8	Ground	
9	Key	No pin
10	TP_USB_ICH_NC	Test point

One low-profile 2x5 connector (J2D2) on the server boards provides an option to support a low-profile USB Solid State Drive.

Table 65. Pin-out of Internal Low-Profile USB Connector for Solid State Drive (J2D2)

Pin	Signal Name	Description
1	USB_PWR11_5V	USB power
2	NC	Not Connected
3	USB Data -	USB port 11 negative signal
4	NC	Not Connected
5	USB Data +	USB port 11 positive signal
6	NC	Not Connected
7	Ground	Ground
8	NC	Not Connected
9	Key	No pin
10	LED#	Activity LED

The server boards provide one additional Type A USB port (J1H2) to support the installation of a USB device inside the server chassis.

Table 66. Internal Type A USB Port Pin-out (J1H2)

Pin	Signal Name	Description
1	USB_PWR7_5V	USB_PWR
2	USB_ICH_P7N	USB port 7 negative signal
3	USB_ICH_P7P	USB port 7 positive signal
4	GND	Ground

6.6 Fan Headers

The server boards provide three SSI-compliant 4-pin and four SSI-compliant 6-pin fan headers to use as CPU and I/O cooling fans. 3-pin fans are supported on all fan headers. 6-pin fans are supported on headers J1K1, J1K2, J1K4, and J1K5. 4-pin fans are supported on headers J1K1, J1K2, J1K4, J1K5, J7K1, J9A2, and J9A3. The pin configuration for each of the 4-pin and 6-pin fan headers is identical and defined in the following tables.

- Two 4-pin fan headers are designated as processor cooling fans:
  - CPU1 fan (J9A2)
  - CPU2 fan (J7K1)
- Four 6-pin fan headers are designated as hot-swap system fans:
  - Hot-swap system fan 1 (J1K1)
  - Hot-swap system fan 2 (J1K4)
  - Hot-swap system fan 3 (J1K2)
  - Hot-swap system fan 4 (J1K5)
- One 4-pin fan header is designated as a rear system fan:
  - System fan 5 (J9A3)

Table 67. SSI 4-pin Fan Header Pin-out (J7K1, J9A2, J9A3)

Pin	Signal Name	Type	Description
1	Ground	GND	Ground is the power supply ground
2	12V	Power	Power supply 12 V
3	Fan Tach	In	FAN_TACH signal is connected to the BMC to monitor the fan speed
4	Fan PWM	Out	FAN_PWM signal to control fan speed

Table 68. SSI 6-pin Fan Header Pin-out (J1K1, J1K2, J1K4, J1K5)

Pin	Signal Name	Type	Description
1	Ground	GND	Ground is the power supply ground
2	12V	Power	Power supply 12 V
3	Fan Tach	In	FAN_TACH signal is connected to the BMC to monitor the fan speed
4	Fan PWM	Out	FAN_PWM signal to control fan speed
5	Fan Presence	In	Indicates the fan is present
6	Fan Fault LED	Out	Lights the fan fault LED

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: ▼

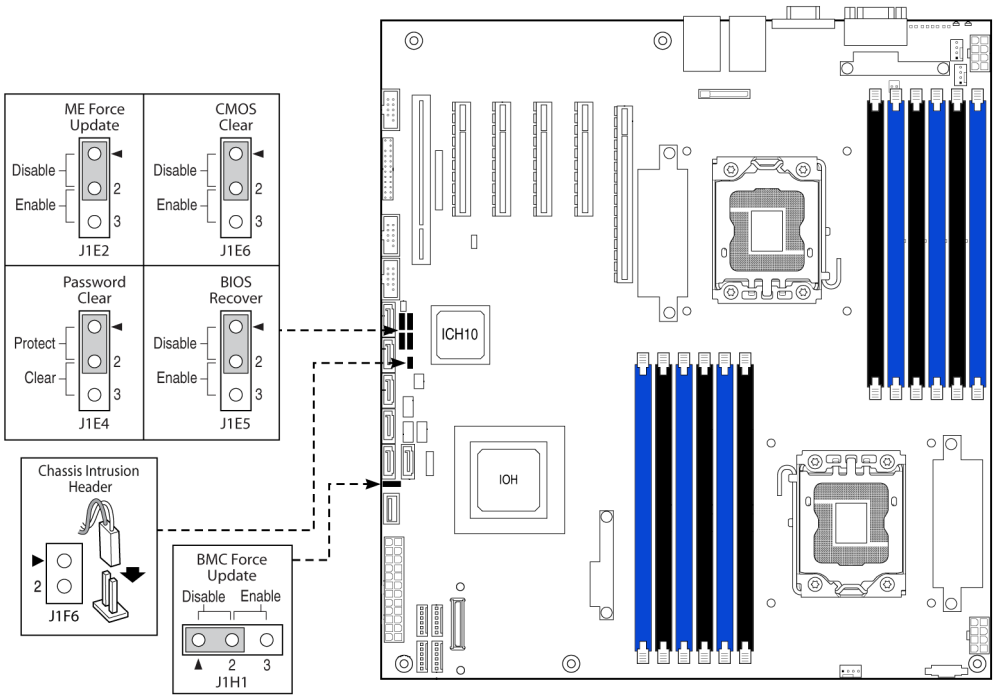


Figure 53. Jumper Blocks (J1E2, J1E4, J1E5, J1E6, J1H1)

Table 69. Server Board Jumpers (J1E6, J1E2, J1E4, J1E5, J1H1)

Jumper Name	Pins	System Results
J1E6: 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.
J1E2: ME Force Update	1-2	ME Firmware Force Update Mode – Disabled **(Default)**
	2-3	ME Firmware Force Update Mode – Enabled
J1E4: 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.
J1E5: 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.
J1H1: Force BMC Update	1-2	BMC Firmware Force Update Mode – Disabled **(Default)**
	2-3	BMC Firmware Force Update Mode – Enabled

7.1 CMOS Clear and Password Reset Usage Procedure

The CMOS Clear (J1E6) and Password Reset (J1E4) 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® server boards. The following procedure outlines the new usage model.

7.1.1 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 (J1E6) 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.

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 (J1E4) 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 (J1H1) 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 (J1H1) 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 Update_Instruction.txt file included in the given 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 (J1H1) 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

1. Power down the system and remove the AC power cord.
2. Open the server chassis. See your server chassis documentation for instructions.
3. Move the BIOS recovery jumper (J1E5) 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 BIOS Recovery procedure as documented in the BIOS release notes.
7. After successful completion of the BIOS recovery, the “BIOS has been updated successfully” message displays.

8. Power down the system and remove the AC power cord.
9. Open the server chassis.
10. Move the BIOS recovery jumper (J1E5) from the “enabled” position (covering pins 2 and 3) to the “disabled” position (covering pins 1 and 2).
11. Close the server chassis.
12. Reconnect the AC power cord and power up the server.

Warning: DO NOT interrupt the BIOS POST during the first boot after the BIOS recovery.

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” include the Integrated BMC, onboard NICs, and optional Intel® RMM3 installed in the Intel® RMM3 slot.

The LED is located near the Intel® SAS Entry RAID Module AXX4SASMOD slot in the lower-left corner of the server boards and is labeled “5VSB_LED”. It 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.

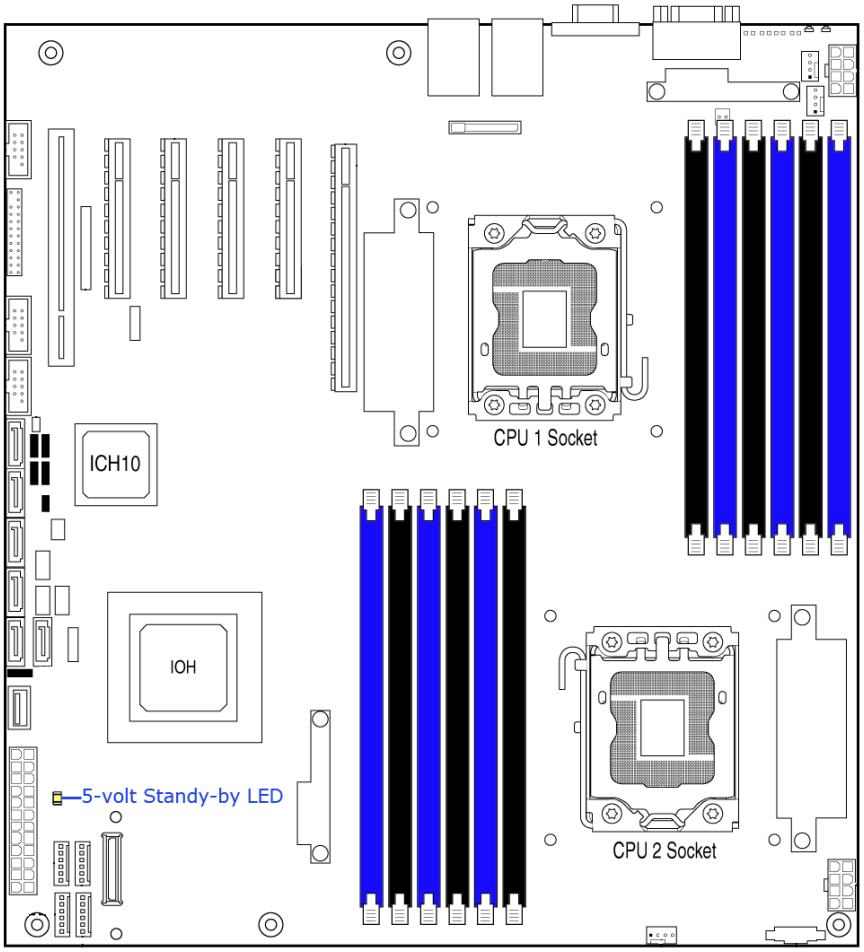


Figure 54. 5-volt Stand-by Status LED Location

8.2 Fan Fault LED's

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.

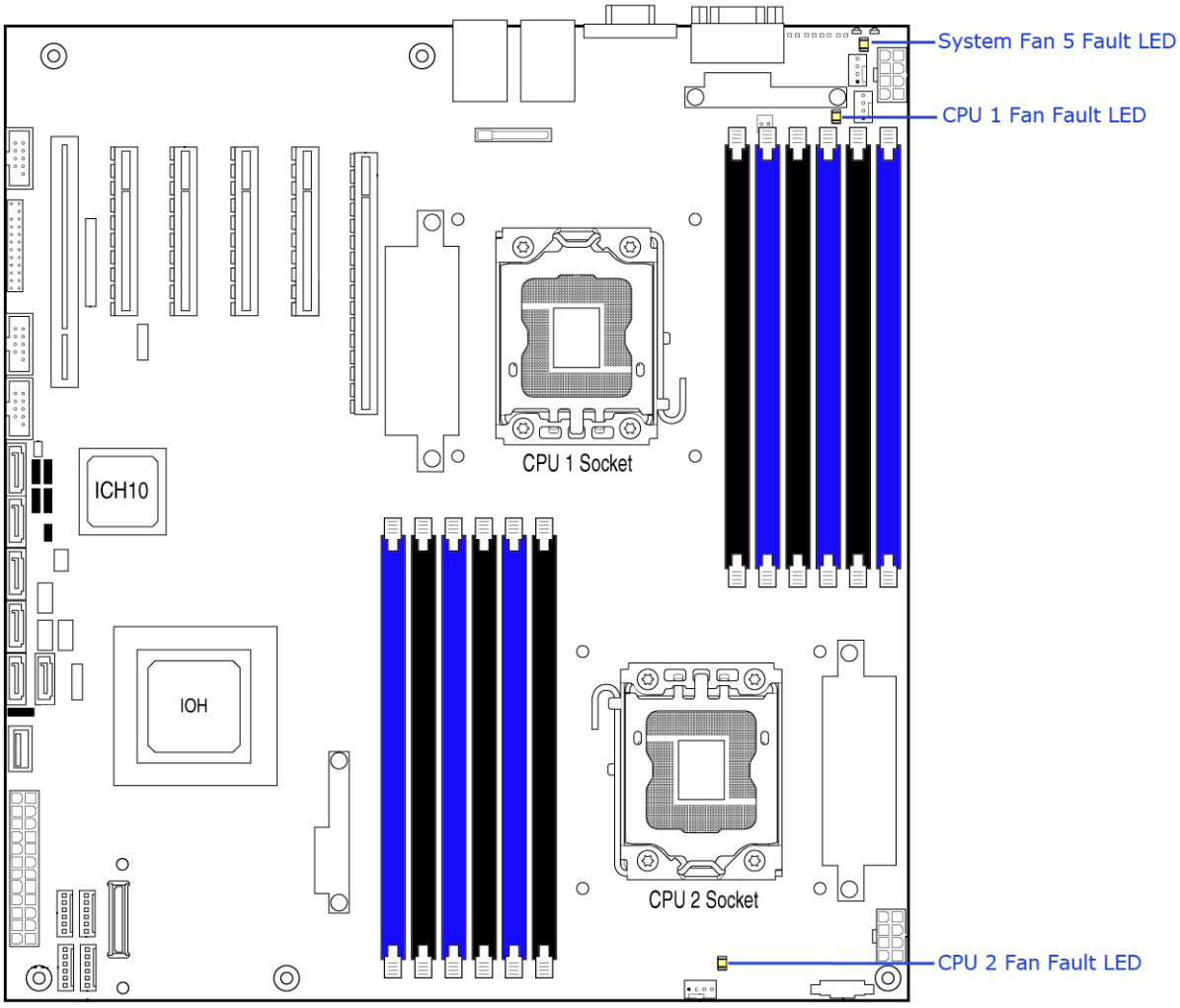
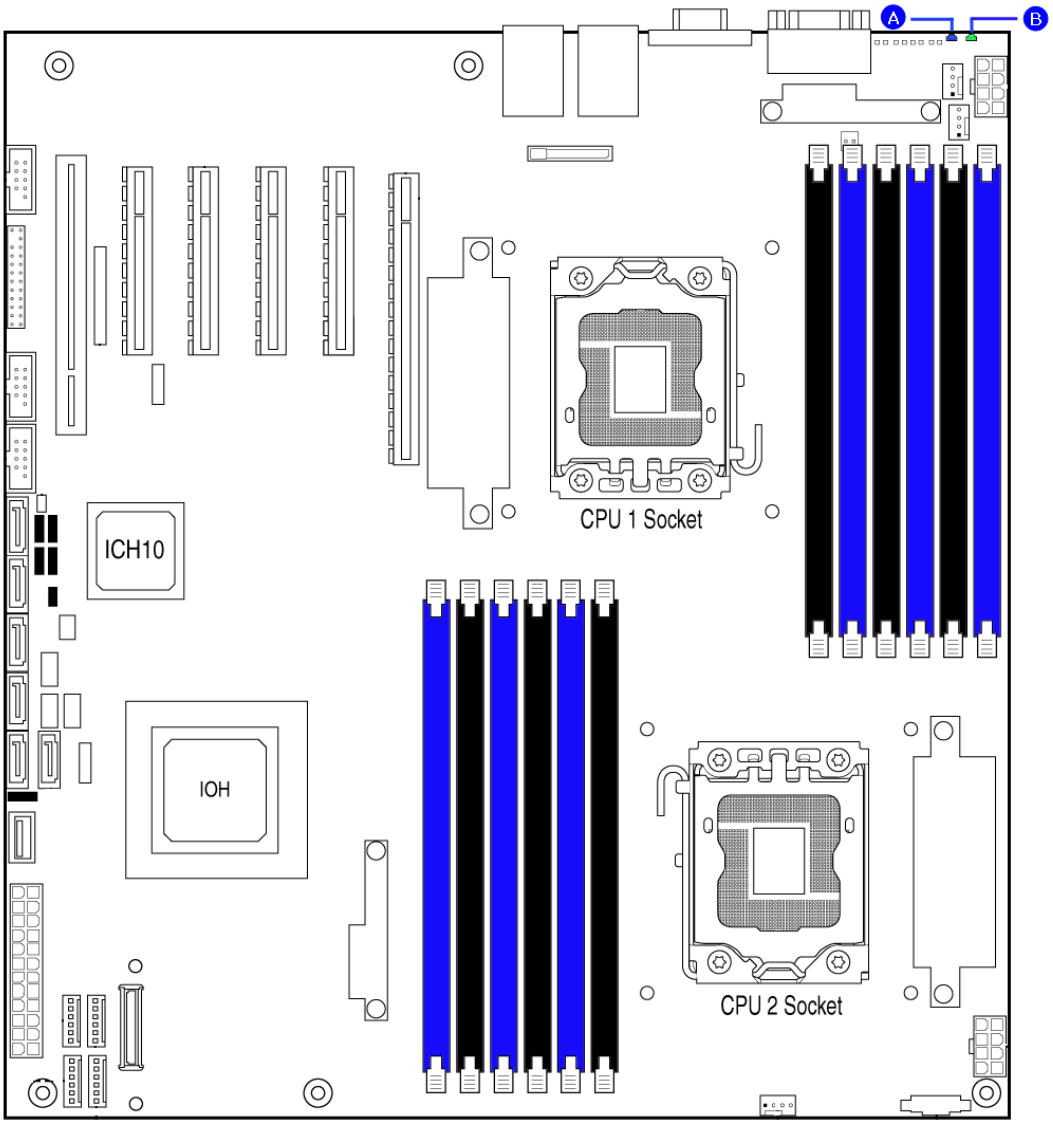


Figure 55. Fan Fault LED's Location

8.3 System ID LED and System Status LED

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



A. System ID LED
B. System Status LED

Figure 56. System Status LED Location

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.

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

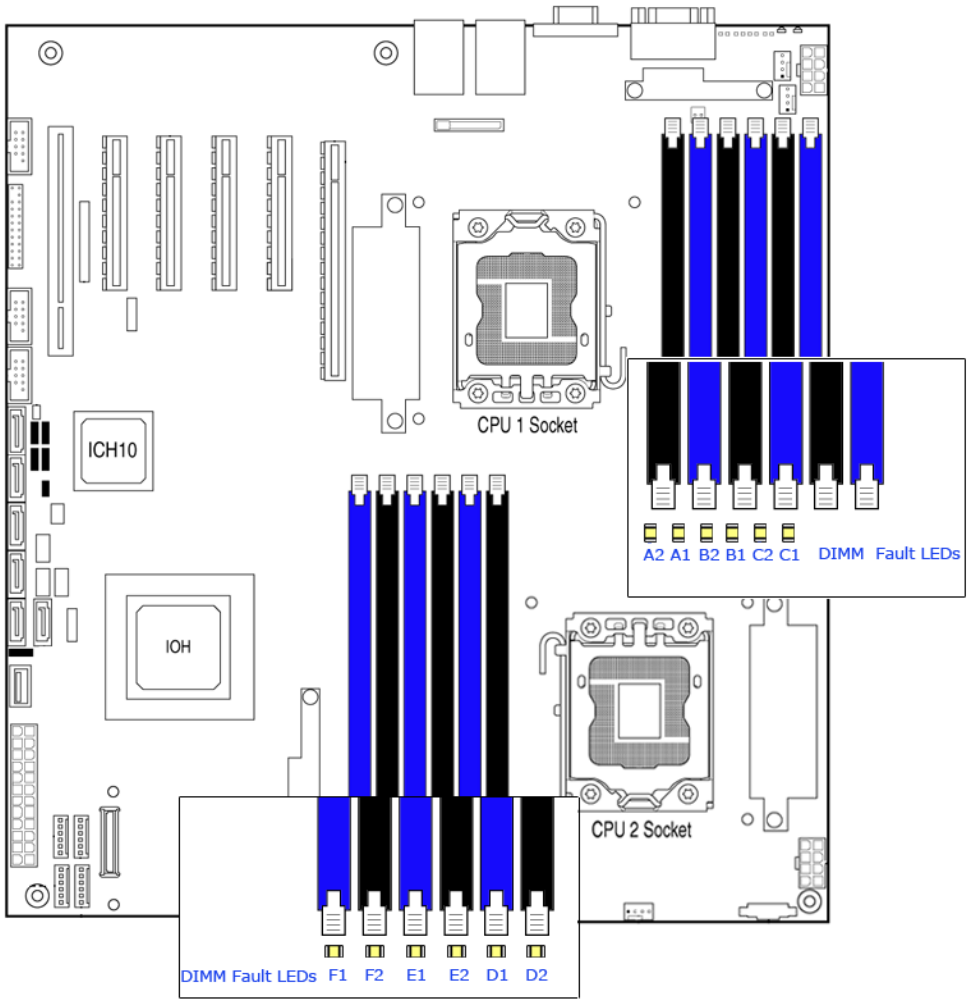
Table 70. System Status LED

Color	State	Criticality	Description
Green	Solid on	System OK	System booted and ready.
Green	Blink	Degraded	System degraded – Non-critical temperature threshold asserted – Non-critical voltage threshold asserted – Non-critical fan threshold asserted – Fan redundancy lost, sufficient system cooling maintained. This does not apply to non-redundant systems. – Power supply predictive failure – Power supply redundancy lost. This does not apply to non-redundant systems. – Correctable errors over a threshold of 10 and migrating to a mirrored DIMM (memory mirroring). This indicates the user no longer has spare DIMMs indicating a redundancy lost condition. The corresponding DIMM LED should light up.
Amber	Blink	Non-critical	Non-fatal alarm – system is likely to fail: – Critical temperature threshold asserted – CATERR asserted – Critical voltage threshold asserted – VRD hot asserted – SMI Timeout asserted
Amber	Solid on	Critical, non-recoverable	Fatal alarm – system has failed or shut down – CPU Missing – Thermal Trip asserted – Non-recoverable temperature threshold asserted – Non-recoverable voltage threshold asserted – Power fault/Power Control Failure – Fan redundancy lost, insufficient system cooling. This does not apply to non-redundant systems. – Power supply redundancy lost insufficient system power. This does not apply to non-redundant systems. **Note:** This state also occurs when AC power is first applied to the system. This indicates the BMC is booting.
Off	N/A	Not ready	– AC power off, if no degraded, non-critical, critical, or non-recoverable conditions exist. – System is powered down or S5 states, if no degraded, non-critical, critical, or non-recoverable conditions exist.

* When the server is powered down (transitions to the DC-off state or S5), the BMC is still on standby power and retains the sensor and front panel status LED state established before the power-down event. If the system status is normal when the system is powered down (the LED is in a solid green state), the system status LED is off.

8.4 DIMM Fault LEDs

The server boards 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.



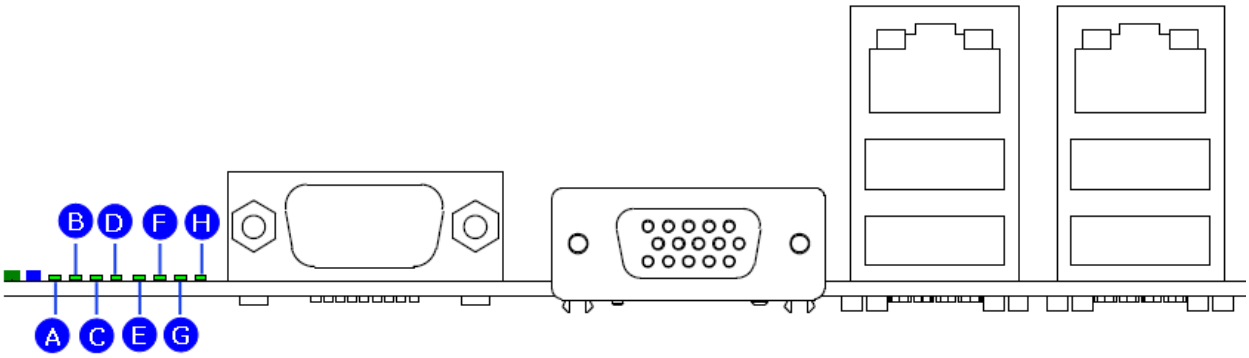
* D2, E2, and F2 DIMM slot and Fault LED's are empty in Intel® Server Board S5500HCV

Figure 57. DIMM Fault LED's Location

8.5 Post Code Diagnostic LEDs

Eight amber POST code diagnostic LEDs are located on the back edge of the server boards in the rear I/O area of the server boards by the serial A connector.

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. See Appendix E for a complete description of how these LEDs are read and a list of all supported POST codes.



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)

Figure 58. POST Code Diagnostic LED Locations

9. Design and Environmental Specifications

9.1 Intel® Server Boards S5520HC, S5500HCV, and S5520HCT Design Specifications

Operation of the Intel® Server Boards S5520HC and/or S5500HCV 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 71. 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, 50 G, 170 inches/sec
Shock (Packaged)	
< 20 pounds	36 inches
20 to < 40 pounds	30 inches
40 to < 80 pounds	24 inches
80 to < 100 pounds	18 inches
100 to < 120 pounds	12 inches
120 pounds	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 1, method I case 3
- Operating Temperature: Server in 30° C ambient air
- Operating Environment: Ground Benign, Controlled

- Duty Cycle: 100%
- Quality Level: II

Table 72. MTBF Estimate

S5520HC MTBF (hours)	S5500HCV MTBF (hours)	Ambient Air Temperature (°C)	Air Temp. at Board for 10(°C) rise (°C)
79,000	89,000	45	55
99,000	111,000	40	50
124,000	140,000	35	45
158,000	178,000	30	40
201,000	227,000	25	35

9.3 Server Board Power Requirements

This section provides power supply design guidelines for a system using the Intel® Server Boards S5520HC, S5500HCV and S5520HCT including voltage and current specifications, and power supply on/off sequencing characteristics. The following diagram shows the power distribution implemented on these server boards.

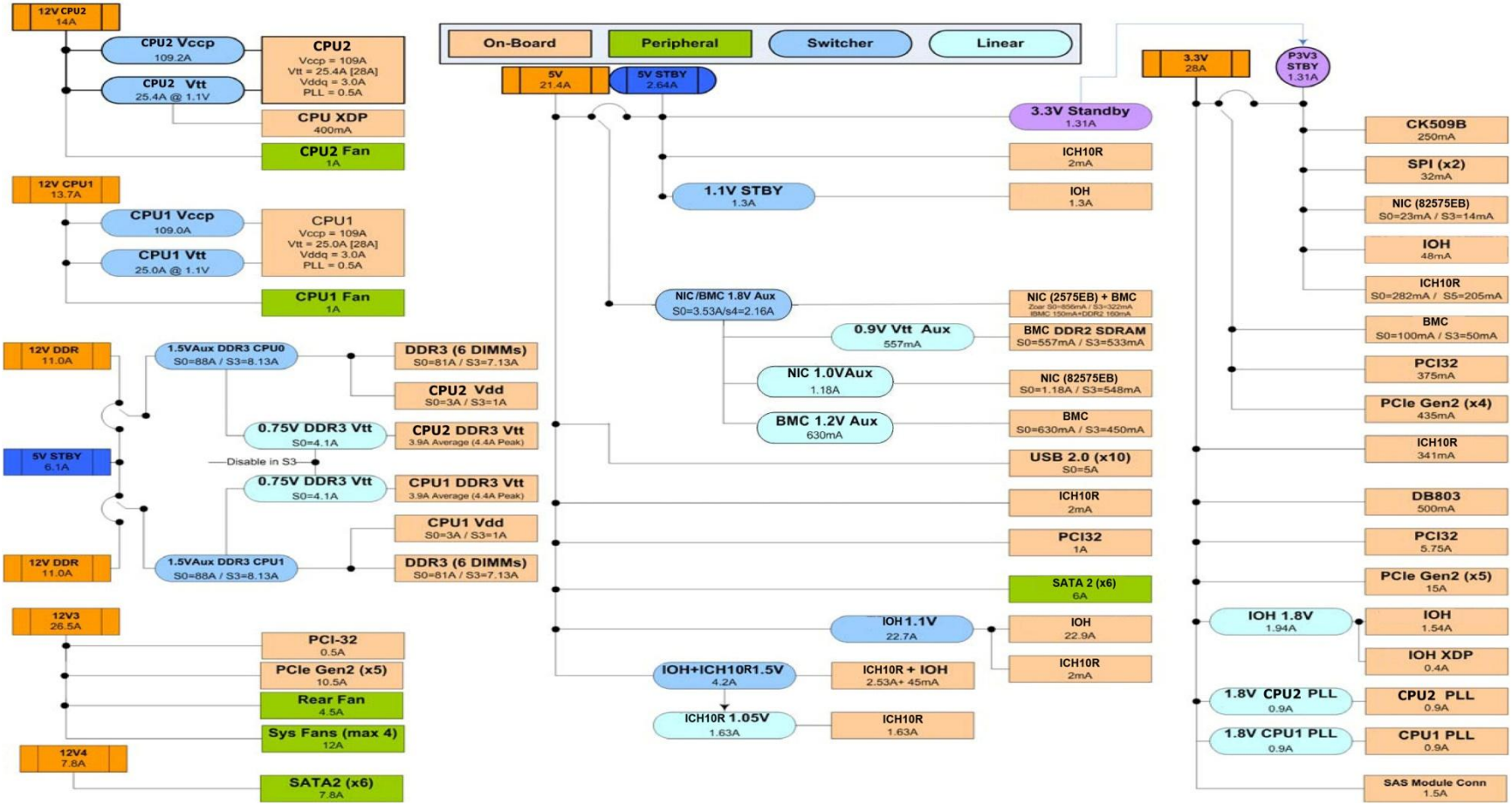


Figure 59. Power Distribution Block Diagram

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) were also followed to determine the suggested thermal and current design values for anticipating future processor needs. The following table provides maximum values for I_{cc}, TDP power and T_{CASE} for the compatible Intel® Xeon® Processor 5500 series.

Table 73. Intel® Xeon® Processor Dual Processor TDP Guidelines

TDP Power	Max Tcase		Icc Max
	Thermal Profile A	Thermal Profile B	
95 W	75 ℃	81 ℃	120 A

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 5U server system.

The combined power of all outputs should not exceed the rated output power of the power supply. The power supply must meet both static and dynamic voltage regulation requirements for the minimum loading conditions.

Table 74. 670-W Load Ratings

Voltage	Minimum Continuous	Maximum Continuous	Peak
+3.3 V	1.0 A	24 A	
+5 V	2.0 A	30 A	
+12 V1	0.5 A	16 A	18 A
+12 V2	1.0 A	16 A	18 A
+12 V3	0.5 A	31 A	33 A
+12 V4	1.0 A	16 A	18 A
-12 V	0 A	0.5 A	
+5 VSB	0.1 A	3.0 A	5 A

1. Maximum continuous total output power must not exceed 670 W.
2. Maximum continuous load on the combined 12-V output must not exceed 48 A.
3. Peak load on the combined 12-V output must not exceed 52 A.
4. Peak total DC output power must not exceed 730 W.
5. For 12 V, peak power and current loading are supported for a minimum of 12 seconds.
6. For 5 VSB, 5 VSB must withstand 5 A for 500 ms under the first turn-on condition.
7. Combined 3.3 V and 5 V power must not exceed 170 W.

9.4.1 Grounding

The output ground of the pins of the power supply provides the output power return path. The output connector ground pins are connected to the safety ground (power supply enclosure).

9.4.2 Stand-by Outputs

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

9.4.3 Remote Sense

The power supply should have remote sense return (ReturnS) to regulate out ground drops for all output voltages: +3.3 V, +5 V, +12 V1, +12 V2, +12 V3, +12 V4, -12 V, and 5 VSB. The power supply should use remote sense to regulate out drops in the system for the +3.3 V, +5 V, and +12 V1 outputs.

The +12 V1, +12 V2, +12 V3, +12 V4, –12 V, and 5V SB outputs only use remote sense referenced to the ReturnS signal. The remote sense input impedance to the power supply must be greater than 200 Ω on 3.3 VS and 5 VS. This is the value of the resistor connecting the remote sense to the output voltage internal to the power supply.

Remote sense must be able to regulate out a minimum of 200 mV drop. The remote sense return (ReturnS) must be able to regulate out a minimum of 20 0mV drop in the power ground return. The current in any remote sense line should be less than 5 mA to prevent voltage sensing errors.

The power supply must operate within specification over the full range of voltage drops from the power supply's output connector to the remote sense points.

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. All outputs are measured with reference to the return remote sense signal (ReturnS). The +12 V3, +12 V4, –12 V and 5 VSB outputs are measured at the power supply connectors referenced to ReturnS. The +3.3 V, +5 V, +12 V1, and +12 V2 are measured at its remote sense signal located at the signal connector.

Table 75. Voltage Regulation Limits

Parameter	Tolerance	Minimum	Nominal	Maximum	Units
+3.3 V	- 5%/+5%	+3.14V	+3.30V	+3.46V	Vrms
+5 V	- 5%/+5%	+4.75V	+5.00V	+5.25V	Vrms
+12 V 1	- 5%/+5%	+11.40V	+12.00V	+12.60V	Vrms
+12 V 2	- 5%/+5%	+11.40V	+12.00V	+12.60V	Vrms
+12 V 3	- 5%/+5%	+11.40V	+12.00V	+12.60V	Vrms
+12 V 4	- 5%/+5%	+11.40V	+12.00V	+12.60V	Vrms
- 12 V	- 5%/+9%	- 11.40V	-12.00V	-13.08V	Vrms
+5 VSB	- 5%/+5%	+4.75V	+5.00V	+5.25V	Vrms

9.4.5 Dynamic Loading

The output voltages remain within limits for the step loading and capacitive loading specified in the following table. You should test the load transient repetition rate between 50 Hz and 5 kHz at duty cycles ranging from 10% to 90%. The load transient repetition rate is only a test specification. The Δ step load may occur anywhere within the minimum load to the maximum load range.

Table 76. Transient Load Requirements

Output	Δ Step Load Size 1	Load Slew Rate	Test Capacitive Load
+3.3 V	7.0 A	0.25A/μsec	4700μF
+5 V	7.0 A	0.25A/μsec	1000μF
+12 V	25 A	0.25A/μsec	4700μF
+5 VSB	0.5 A	0.25A/μsec	20μF

1. Step loads on each 12 V output may happen simultaneously.

9.4.6 Capacitive Loading

The power supply should be stable and meet all requirements within the following capacitive loading range.

Table 77. Capacitive Loading Conditions

Output	Minimum	Maximum	Units
+3.3V	250	6800	μF
+5V	400	4700	μF
+12V1, +12V2, +12V3, +12V4	500 each	11,000	μF
-12V	1	350	μF
+5VSB	20	350	μF

9.4.7 Ripple/Noise

The maximum allowed ripple/noise output of the power supply is defined in the following table. This is measured over a bandwidth of 0 Hz to 20 MHz at the power supply output connectors. A 10 μF tantalum capacitor in parallel with a 0.1 μF ceramic capacitor are placed at the point of measurement.

Table 78. Ripple and Noise

+3.3V	+5V	+12V1, +12V2, +12V3, +12V4	-12V	+5 VSB
50 mVp-p	50 mVp-p	120 mVp-p	120 mVp-p	50 mVp-p

9.4.8 Timing Requirements

The following are the timing requirements for the power supply operation. The output voltages must rise from 10% to within regulation limits (T_{vout_rise}) within 5 ms to 70 ms. 5 VSB is allowed to rise from 1.0 ms to 25 ms. +3.3 V, +5 V, and +12 V output voltages should start to rise approximately at the same time. All outputs must rise monotonically. Each output voltage should reach regulation within 50 ms (T_{vout_on}) of each other during turn on of the power supply. Each output voltage should fall out of regulation within 400 msec (T_{vout_off}) of each other during turn off.

The following tables and diagrams show the timing requirements for the power supply being turned on and off via the AC input with PSON held low, and the PSON signal with the AC input applied.

Table 79. Output Voltage Timing

Item	Description	Minimum	Maximum	Units
Tvout_rise	Output voltage rise time from each main output.	5.0 1	70 1	ms
Tvout_rise	All main outputs must be within regulation of each other within this time.	N/A	50	ms
Tvout_rise	All main outputs must leave regulation within this time.	N/A	400	ms

1. The 5 VSB output voltage rise time is from 1.0 ms to 25 ms

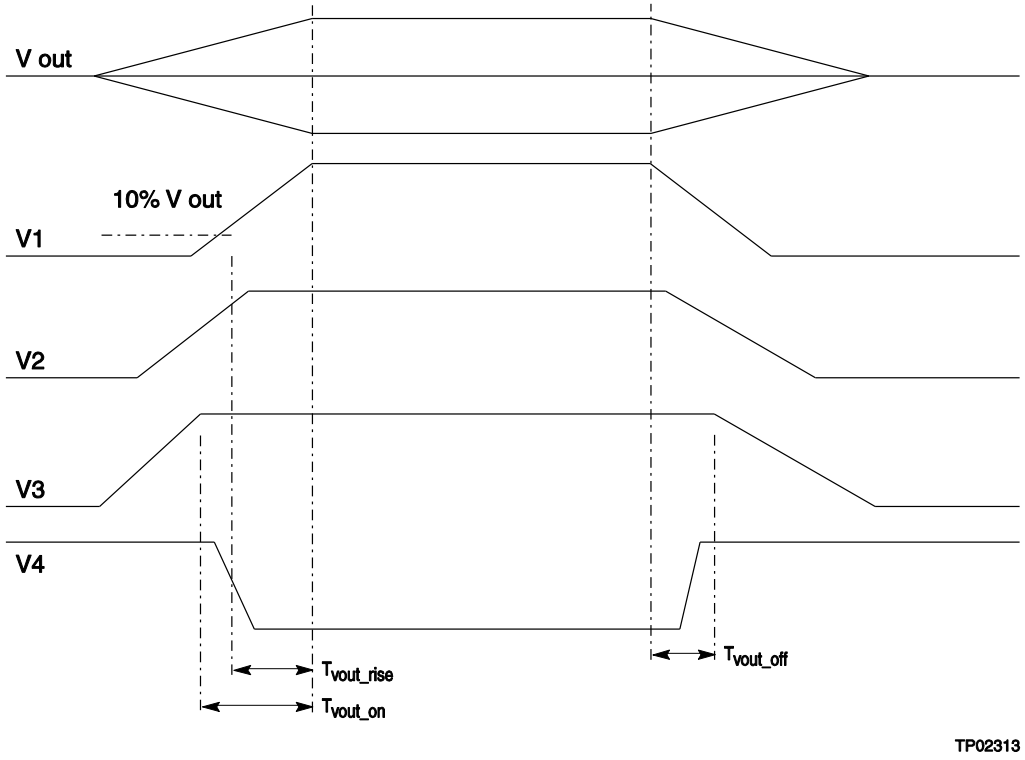


Figure 60. Output Voltage Timing

Table 80. Turn On/Off Timing

Item	Description	Minimum	Maximum	Units
Tsb_on_delay	Delay from AC being applied to 5 VSB being within regulation.	N/A	1500	ms
Tac_on_delay	Delay from AC being applied to all output voltages being within regulation.	N/A	2500	ms
Tvout_holdup	Time all output voltages stay within regulation after loss of AC.	21	N/A	ms
Tpwok_holdup	Delay from loss of AC to de-assertion of PWOK	20	N/A	ms
Tpson_on_delay	Delay from PSON# active to output voltages within regulation limits.	5	400	ms
Tpson_pwok	Delay from PSON# deactivate to PWOK being de-asserted.		50	ms
Tpwok_on	Delay from output voltages within regulation limits to PWOK asserted at turn on.	100	500	ms
Tpwok_off	Delay from PWOK de-asserted to output voltages (3.3 V, 5 V, 12 V, and -12 V) dropping out of regulation limits.	1	N/A	ms
Tpwok_low	Duration of PWOK being in the de-asserted state during an off/on cycle using AC or the PSON signal.	100	N/A	ms
Tsb_vout	Delay from 5 VSB being in regulation to O/Ps being in regulation at AC turn on.	50	1000	ms
T5VSB_holdup	Time the 5 VSB output voltage stays within regulation after loss of AC.	70	N/A	ms

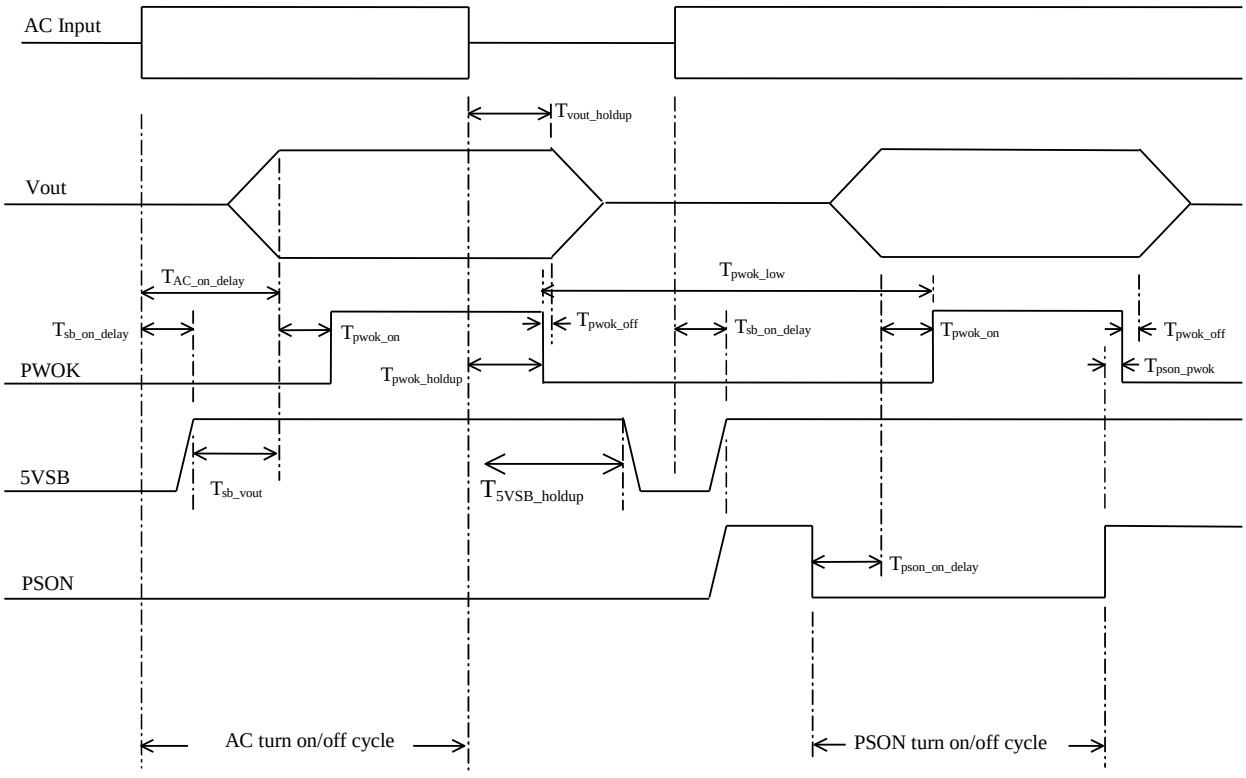


Figure 61. Turn On/Off Timing (Power Supply Signals)

9.4.9 Residual Voltage Immunity in Stand-by Mode

The power supply should be immune to any residual voltage placed on its outputs (typically, a leakage voltage through the system from stand-by output) up to 500 mV. There should be no additional heat generated or stressing of any internal components with this voltage applied to any individual output and all outputs simultaneously. It also should not trip the power supply protection circuits during turn on.

Residual voltage at the power supply outputs for a no-load condition should not exceed 100 mV when AC voltage is applied and the PSON# signal is de-asserted.

10. Regulatory and Certification Information

To help ensure EMC compliance with your local regional rules and regulations, before computer integration, make sure that the chassis, power supply, and other modules have passed EMC testing using a server board with a microprocessor from the same family (or higher) and operating at the same (or higher) speed as the microprocessor used on this server board. The final configuration of your end system product may require additional EMC compliance testing. For more information, please contact your local Intel Representative.

This is an FCC Class A device. Integration of it into a Class B chassis does not result in a Class B device.

10.1 Product Regulatory Compliance

Intended Application – This product was evaluated as Information Technology Equipment (ITE), which may be installed in offices, schools, computer rooms, and similar commercial type locations. The suitability of this product for other product categories and environments (such as: medical, industrial, telecommunications, NEBS, residential, alarm systems, test equipment, etc.), other than an ITE application, may require further evaluation.

10.1.1 Product Safety Compliance

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT comply with the following safety requirements:

- UL60950 - CSA 60950 (USA/Canada)
- EN60950 (Europe)
- IEC60950 (International)
- CB Certificate & Report, IEC60950 (report to include all country national deviations) GS License (Germany)
- GOST R 50377-92 - License (Russia) – Listed on System License
- Belarus License (Belarus) – Listed on System License
- CE - Low Voltage Directive 73/23/EEE (Europe)
- IRAM Certification (Argentina)

10.1.2 Product EMC Compliance – Class A Compliance

The Intel® Server Boards S5520HC, S5500HCV and S5520HCT have been tested and verified to comply with the following electromagnetic compatibility (EMC) regulations when installed a compatible Intel® host system. For information on compatible host system(s) refer to http://support.intel.com/support/motherboards/server/S5520HC/ or contact your local Intel representative.

- FCC /ICES-003 - Emissions (USA/Canada) Verification
- CISPR 22 – Emissions (International)
- EN55022 - Emissions (Europe)
- EN55024 - Immunity (Europe)
- CE – EMC Directive 89/336/EEC (Europe)
- AS/NZS 3548 Emissions (Australia/New Zealand)
- VCCI Emissions (Japan)

- BSMI CNS13438 Emissions (Taiwan)
- RRL Notice No. 1997-41 (EMC) & 1997-42 (EMI) (Korea)
- GOST R 29216-91 Emissions (Russia) – Listed on System License
- GOST R 50628-95 Immunity (Russia) – Listed on System License
- Belarus License (Belarus) – Listed on System License

10.1.3 Certifications/Registrations/Declarations

- UL Certification or NRTL (US/Canada)
- CB Certifications (International)
- CE Declaration of Conformity (CENELEC Europe)
- FCC/ICES-003 Class A Attestation (USA/Canada)
- C-Tick Declaration of Conformity (Australia)
- MED Declaration of Conformity (New Zealand)
- BSMI Certification (Taiwan)
- RRL KCC Certification (Korea)
- Ecology Declaration (International)

10.2 Product Regulatory Compliance Markings

Regulatory Compliance	Country	Marking
UL Mark	USA/Canada	
CE Mark	Europe	
EMC Marking (Class A)	Canada	CANADA ICES-003 CLASS A CANADA NMB-003 CLASSE A
BSMI Marking (Class A)	Taiwan	 警告使用者： 這是甲類的資訊產品，在居住的環境中使用時， 可能會造成射頻干擾，在這種情況下，使用者會 被要求採取某些適當的對策
C-tick Marking	Australia/New Zealand	
RRL KCC Mark	Korea	 방송통신위원회
EFUP Mark	China	
Country of Origin	Exporting Requirements	Made in xxxxx
Model Designation	Regulatory	Examples (Server Board S5520HC) for boxed type boards; or Board

	Identification	PB number for non-boxed boards (typically high-end boards)

10.3 Electromagnetic Compatibility Notices

FCC (USA)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions related to the EMC performance of this product, contact:

Intel Corporation
5200 N.E. Elam Young Parkway
Hillsboro, OR 97124-6497
1-800-628-8686

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit other than the one to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment. The customer is responsible for ensuring compliance of the modified product.

Only peripherals (computer input/output devices, terminals, printers, etc.) that comply with FCC Class A or B limits may be attached to this computer product. Operation with noncompliant peripherals is likely to result in interference to radio and TV reception.

All cables used to connect to peripherals must be shielded and grounded. Operation with cables, connected to peripherals that are not shielded and grounded may result in interference to radio and TV reception.

ICES-003 (Canada)

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans lanorme sur le matériel brouilleur: “Apparelis Numériques”, NMB-003 édictee par le Ministre Canadian des Communications.

English translation of the notice above:

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled: “Digital Apparatus,” ICES-003 of the Canadian Department of Communications.

Europe (CE Declaration of Conformity)

This product has been tested in accordance too, and complies with the Low Voltage Directive (73/23/EEC) and EMC Directive (89/336/EEC). The product has been marked with the CE Mark to illustrate its compliance.

VCCI (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

English translation of the notice above:

This is a Class B product based on the standard of the Voluntary Control Council for Interference (VCCI) from Information Technology Equipment. If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

BSMI (Taiwan)

The BSMI Certification Marking and EMC warning is located on the outside rear area of the product.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策

RRL KCC (Korea)

10.4 Product Ecology Change (EU RoHS)

Intel has a system in place to restrict the use of banned substances in accordance with the European Directive 2002/95/EC. Compliance is based on declaration that materials banned in the RoHS Directive are either (1) below all applicable threshold limits or (2) an approved/pending RoHS exemption applies.

RoHS implementation details are not fully defined and may change.

Threshold limits and banned substances are noted below:

- Quantity limit of 0.1% by mass (1000PPM) for:
  - Lead
  - Mercury
  - Hexavalent Chromium
  - Polybrominated Biphenyls Diphenyl Ethers (PBDE)
- Quantity limit of 0.01% by mass (100 PPM) for:
  - Cadmium

10.5 Product Ecology Change (CRoHS)

CRoHS (China RoHS, or Ministry of Information Industry Order #39, "Management Methods for Controlling Pollution by Electronic Information Products."):

- China bans the same substances and limits as noted for EU RoHS; however require product marking and controlled substance information Environmental Friendly Usage Period (EFUP) Marking Is defined in number of years in which controlled listed substances will not leak or chemically deteriorate while in the product. Intel understands the end-seller (entity placing product into market place) is responsible for providing EFUP marking.
- Intel "retail" products are provided with EFUP marking
- For "Business to Business" products, Intel intends to place EFUP marking on product for customer convenience
- EFUP for Intel server products has been determined as 20 years.

Below is an example of EFUP mark applied to Intel server products.

CRoHS Substance Tables:

China CRoHS requires products to be provided with controlled substance information. Intel understands the end-seller (entity placing product into market place) is responsible for providing the controlled substance information. Controlled substance information is required to be in Simplified Chinese. Substance table for this board product is as follows:

关于符合中国《电子信息产品污染控制管理办法》的声明

Management Methods on Control of Pollution from

Electronic Information Products

(China RoHS declaration)

产品中有毒有害物质的名称及含量

部件名称 (Parts)	有毒有害物质或元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr6+)	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件 Metal Parts	○	○	○	×	○	○
印刷板组件 Printed Board Assemblies (PBA)	×	○	○	○	○	○

○：表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363-2006 标准规定的限量要求以下。

○：Indicates that this hazardous substance contained in all homogeneous materials of this part is below the limit requirement in SJ/T 11363-2006.

×：表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363-2006 标准规定的限量要求。

×：Indicates that this hazardous substance contained in at least one of the homogeneous materials of this part is above the limit requirement in SJ/T 11363-2006.

对销售之日的所售产品,本表显示我公司供应链的电子信息产品可能包含这些物质。注意：在所售产品中可能会也可能不会含有所有所列的部件

This table shows where these substances may be found in the supply chain of our electronic information products, as of the date of sale of the enclosed product. Note that some of the component types listed above may or may not be a part of the enclosed product.

10.6 China Packaging Recycle Marks (or GB18455-2001)

Intel EPSD has the following ecological compliances:

Cardboard and fiberboard packaging will be marked as recyclable in China.

China Packaging Recycling Marks is required on retail packaging to be marked as recyclable using China's recycling logo. Due to regional variances in mark acceptances, all three marks accepted worldwide will be implemented on Intel's cardboard and fiberboard. Examples of marks are shown below.

10.7 CA Perchlorate Warning

CA Lithium Perchlorate Warning (California Code of Regulations, Title 22, Division 4.5, Chapter 33: Best Management Practices for Perchlorate Materials):

The State of California requires a warning to be included for products containing a device using Lithium Perchlorate.

Intel understands CA Lithium Perchlorate require a printed warning to be included with all products containing a Lithium battery, either as an insert, in existing product literature, or as part of the shipping memo wording.

Wording is as follows:

Perchlorate Material - special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate.

This notice is required by California Code of Regulations, Title 22, Division 4.5, Chapter 33: Best Management Practices for Perchlorate Materials. This product/part includes a battery that contains Perchlorate material.

10.8 End-of-Life/Product Recycling

Product recycling and end-of-life take-back systems and requirements vary by country.

Contact the retailer or distributor of this product for information about product recycling and/or take-back.

Appendix A: Integration and Usage Tips

- Prior to adding or removing components or peripherals from the server board, you must remove the AC power cord. 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 Intel® Xeon® Processor 5500 Series only. This server board does not support previous generation Intel® Xeon® processors.
- You must install processors in order. CPU 1 socket is located near the back edge of the server board and must be populated to operate the board and enable CPU 2 socket.
- On the back edge of the server board, there are EIGHT diagnostic LEDs that display a sequence of amber POST codes during the boot process. If the server board hangs during POST, the LEDs display the last POST event run before the hang.
- Only Registered DDR3 DIMMs (RDIMMs) and Unbuffered DDR3 DIMMs (UDIMMs) are supported on this server board. Mixing of RDIMMs and UDIMMs is not supported.
- Must always start populating DDR3 DIMMs in the first slot on each memory channel (Memory slot A1, B1, C1, D1, E1, or F1)
- Must populate Quad-Rank RDIMM starting with the first slot (Memory slot A1, B1, C1, D1, E1, or F1) on each memory channel.
- For the best performance, you should balance the number of DDR3 DIMMs installed across both processor sockets and memory channels. For example: with two processors installed, a 6-DIMM configuration with identical DIMMs in slot A1, B1, C1, D1, E1, and F1 performs better than a 6-DIMM configuration with identical DIMMs at A1, A2, B1, B2, C1, and C2.
- The Intel® RMM3 connector is not compatible with the Intel® Remote Management Module (Product Code AXXRMM) or the Intel® Remote Management Module 2 (Product Code AXXRMM2).
- Normal BMC functionality is disabled with the Force BMC Update jumper (J1H1) set to the “enabled” position (pins 2-3). You should never run the server with the Force BMC Update jumper set in this position and should only use the jumper in this position when the standard BMC firmware update process fails. This jumper must remain in the default (disabled) position (pins 1-2) when the server is running normally.
- This server board no longer supports the Rolling BIOS (two BIOS banks). It implements the BIOS Recovery mechanism instead.
- When performing a normal BIOS update procedure, you must set the BIOS Recovery jumper (J1E5) to its default position (pins 1-2).
- Locate the device that generates System Event Log (SEL) PCI device event: the SEL PCI device event may not specify which PCI device in the system that generates the event entry, users can follow below tips to locate the PCI device:
  - Step1: Identify the PCI device location number: the SEL event entry in Hex code (see the SEL viewer utility help text instruction for read of Hex code) provides the PCI device bus number, device number, and function number with last two bytes: ED2 and ED3. The byte of ED2 provides the PCI device bus number; the higher four bits of ED3 byte provides the device number, and the lower four bits of ED3 byte provides the function number.

- Step 2: Decide the PCI device with location number (Bus number, Device number, and Function number) using PCI map dump from the system generating the PCI device SEL event, There are multiple means to dump the PCI map. For example, read the location number from the device general property page in device manager under Microsoft Windows* Operating Systems, or type 'PCI' and execute under the server board EFI shell
- Example of deciding the PCI device that generates SEL event entry: 1) Provided a PCI device SEL event entry in Hex code reads the ED2 as 01 and ED3 as 00, that is, the PCI device has bus number=1, device number=0, and function number=0; 2) The PCI dump from this system indicates the device with bus number=1, device number=0, and function number=0 as "Network Controller - Ethernet controller" and there is no add-in NIC inserted, thus the PCI device generate the SEL event entry is onboard NIC controller.

Appendix B: Compatible Intel® Server Chassis

Refer to the following table for the compatible Intel® Server Chassis of Intel® Server Boards S5520HC, S5500HCV and S5520HCT:

Passive tower processor heatsink(s) (product code: FXXRGTHSINK) is required when installing the Intel® Server Board S5520HC or S5500HCV in the Intel® Server Chassis SC5600LX.

Active processor heatsink(s) is required when installing the Intel® Server Board S5520HC or S5500HCV in any of following Intel® Server Chassis:

- Intel® Server Chassis SC5600Base
- Intel® Server Chassis SC5600BRP
- Intel® Server Chassis SC5650DP
- Intel® Server Chassis SC5650BRP

Table 81. Compatible Chassis/Heatsink Matrix

S5520HC	S5500HCV	Chassis SKU	Heatsink Includes	Intel® Thermal Solution STS100C (w/ fan, Active mode)	Intel® Thermal Solution STS100A (Active)	FXXRGTHSINK (Passive Tower Heatsink)
Y	Y	**SC5600Base**	No	Y	Y	N
Y	Y	**SC5600BRP**	No	Y	Y	N
Y	Y	**SC5600LX**	No	N	N	Required
Y	Y	**SC5650DP**	No	Y	Y	N
Y	Y	**SC5650BRP**	No	Y	Y	N
Y: Support **N: Not Support**			**Maximum CPU Power Support in Intel Server**	95 W	80 W	95 W

S5520HC	S5500HCV	Chassis SKU	Heatsink Includes	Intel® Thermal Solution STS100C (w/ fan, Active mode)	Intel® Thermal Solution STS100A (Active)	FXXRGTHSINK (Passive Tower Heatsink)
			Chassis			
			Boxed Product Code	BXSTS100C	BXSTS100A	FXXRGTHSINK
						

Note: Must install active processor heatsink with the airflow direction as shown in the following figure when installing in a compatible Intel® Server Chassis.

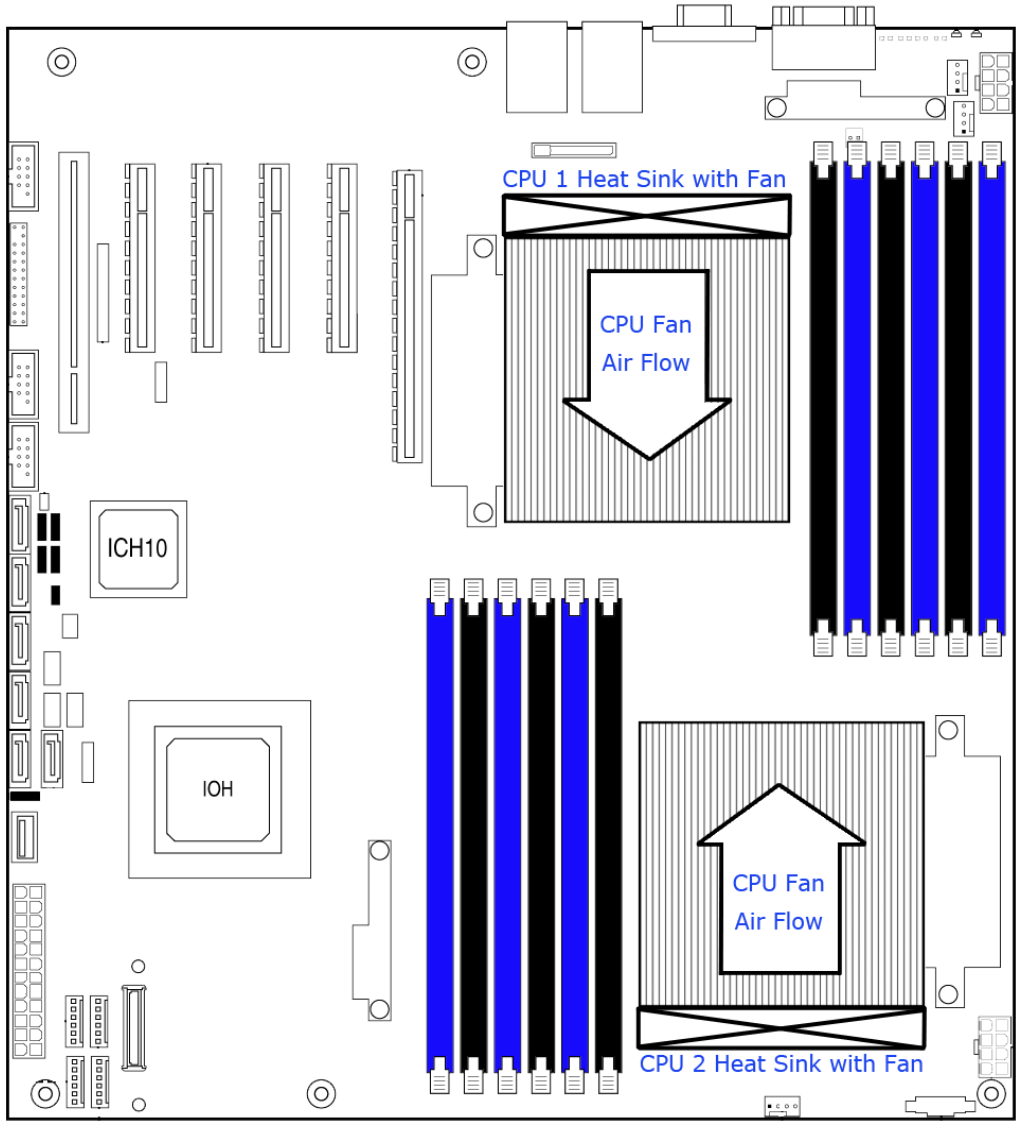


Figure 62. Active Processor Heatsink Installation Requirement

Appendix C: 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**

  The Sensor Type references the values in the sensor type codes table in the *Intelligent Platform Management Interface Specification, Version 2.0* for sensor and event/reading-type table information.

- **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 a specific type of discrete sensors that only have two states.

- **Event Offset/Triggers**

  Event Thresholds are event-generating thresholds 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. You can find the offsets 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/De-assertion Enables**

  Assertion and de-assertion indicators reveal the type of events the sensor generates:

  - As: Assertions
  - De: De-assertion

- **Readable Value/Offsets**

  - Readable Values indicate the type of value returned for threshold and other non-discrete type sensors.
  - Readable Offsets indicate the offsets for discrete sensors that are readable with the *Get Sensor Reading* command. Unless otherwise indicated, all event triggers are readable; Readable Offsets consist of the reading type offsets that do not generate events.

- **Event Data**

  Event data is the data included in an event message generated by the sensor. For threshold-based sensors, the following abbreviations are used:

  - R: Reading value
  - T: Threshold value

- **Rearm Sensors**

  The rearm is a request for the event status of a sensor to be rechecked and updated upon a transition between good and bad states. You can rearm the sensors manually or automatically. This column indicates the type supported by the sensor. These 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 is 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 Control Panel Status LED.

- **Standby**

  Some sensors operate on standby power. You can access these sensors and/or generate events when the main (system) power is off but AC power is present.

Table 82. 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 04 - A/C lost	OK	As and De	–	Trig Offset	A	X
					05 - Soft power control failure 06 - Power unit failure	Fatal					
Power Unit Redundancy1 *(Pwr Unit Redund)*	02h	Chassis-specific	Power Unit 09h	Generic 0Bh	00 - Fully Redundant	OK	As and De	–	Trig Offset	A	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					

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
					06 – Redundant: degraded from fully redundant state.	Degraded					
					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	OK	As and De	–	Trig Offset	A	X
					04 - LAN leash lost	OK					
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	04 – PEF action	OK	As	-	Trig Offset	A,I	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
BB +1.1V IOH *(BB +1.1V IOH)*	10h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
BB +1.1V P1 Vccp *(BB +1.1V P1 Vccp)*	11h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
BB +1.1V P2 Vccp *(BB +1.1V P2 Vccp)*	12h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
BB +1.5V P1 DDR3 *(BB +1.5V P1 DDR3)*	13h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
BB +1.5V P2 DDR3 *(BB +1.5V P2 DDR3)*	14h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
BB +1.8V AUX *(BB +1.8V AUX)*	15h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
BB +3.3V *(BB +3.3V)*	16h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
BB +3.3V STBY *(BB +3.3V STBY)*	17h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
BB +3.3V Vbat *(BB +3.3V Vbat)*	18h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
BB +5.0V *(BB +5.0V)*	19h	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
BB +5.0V STBY *(BB +5.0V STBY)*	1Ah	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
BB +12.0V *(BB +12.0V)*	1Bh	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
BB -12.0V *(BB -12.0V)*	1Ch	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–
Baseboard Temperature *(Baseboard Temp)*	20h	All	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
IOH Thermal Margin *(IOH Therm Margin)*	22h	All	Temperature 01h	Threshold 01h	–	–	–	Analog	–	–	–
Processor 1 Memory Thermal Margin *(Mem P1 Thrm Mrgn)*	23h	All	Temperature 01h	Threshold 01h	–	–	–	Analog	–	–	–
Processor 2 Memory Thermal Margin *(Mem P2 Thrm Mrgn)*	24h	Dual processor only	Temperature 01h	Threshold 01h	–	–	–	Analog	–	–	–
Fan Tachometer Sensors *(Chassis specific sensor names)*	30h–39h	Chassis-specific	Fan 04h	Threshold 01h	[l] [c,nc]	nc = Degraded c = Non-fatal2	As and De	Analog	R, T	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
Fan Present Sensors *(Fan x Present)*	40h–45h	Chassis-specific	Fan 04h	Generic 08h	01 - Device inserted	OK	As and De	-	Triggered Offset	Auto	–
Fan Redundancy [1] *(Fan Redundancy)*	46h	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					

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 degraded from non-redundant	Degraded					
Power Supply 1 Status *(PS1 Status)*	50h	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 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)*	52h	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)*	53h	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 %)*	54h	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 %)*	55h	Chassis-specific	Current 03h	Threshold 01h	[u] [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
Power Supply 1 Temperature *(PS1 Temperature)*	56h	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)*	57h	Chassis-specific	Temperature	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Processor 1 Status *(P1 Status)*	60h	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)*	61h	Dual processor only	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)*	62h	All	Temperature 01h	Threshold 01h	–	–	–	Analog	–	–	–
Processor 2 Thermal Margin *(P2 Therm Margin)*	63h	Dual processor only	Temperature 01h	Threshold 01h	–	–	–	Analog	–	–	–
Processor 1 Thermal Control % *(P1 Therm Ctrl %)*	64h	All	Temperature 01h	Threshold 01h	[u] [c,nc]	Non-fatal	As and De	Analog	Trig Offset	A	–
Processor 2 Thermal Control % *(P2 Therm Ctrl %)*	65h	Dual processor only	Temperature 01h	Threshold 01h	[u] [c,nc]	Non-fatal	As and De	Analog	Trig Offset	A	–
Processor 1 VRD Temp *(P1 VRD Hot)*	66h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Fatal	As and De	–	Trig Offset	M	–
Processor 2 VRD Temp *(P2 VRD Hot)*	67h	Dual processor only	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	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
Catastrophic Error *(CATERR)*	68h	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	Non-fatal	As and De	–	Trig Offset	M	–
CPU Missing *(CPU Missing)*	69h	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	M	–
IOH Thermal Trip *(IOH Thermal Trip)*	6Ah	All	Temperature 01h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	M	–

Note 1: Sensor only present on systems that have applicable redundancy (for instance, a fan or power supply).

Appendix D: Platform Specific BMC Appendix

Table 83. Platform Specific BMC Features

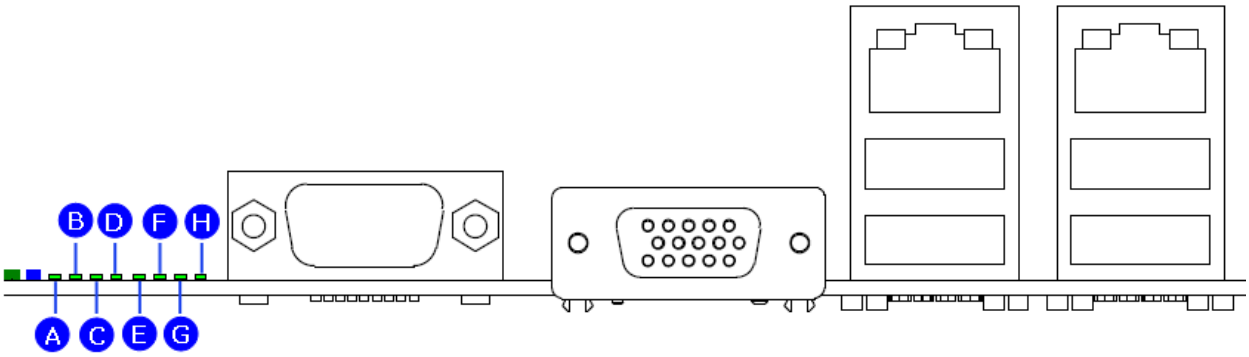
Y: Support **N:** Not Support		Intel® Server Chassis SC5650DP	Intel® Server Chassis SC5650BRP	Intel® Server Chassis SC5600Base	Intel® Server Chassis SC5600BRP	Intel® Server Chassis SC5600LX
Intel® Server Board S5520HC		Compatible	Compatible	Compatible	Compatible	Compatible
Intel® Server Board S5500HCV		Compatible	Compatible	Compatible	Compatible	Compatible
Fan Tachometer Sensors	CPU 1 Fan Sensor #31	Y	Y	Y	Y	N
	CPU 2 Fan Sensor #30	Y	Y	Y	Y	N
	System Fan 1 Sensor #37	Y	Y	Y	Y	Y
	System Fan 2 Sensor #36	N	N	N	N	Y
	System Fan 3 Sensor #35	Y	Y	Y	Y	Y
	System Fan 4 Sensor #34	N	N	N	N	Y
	System Fan 5 Sensor #33	Y	Y	Y	Y	N
Fan Presence Sensors	System Fan 1 Presence Sensor #40	N	N	N	N	Y
	System Fan 2 Presence Sensor #41	N	N	N	N	Y
	System Fan 3 Presence Sensor #42	N	N	N	N	Y
	System Fan 4 Presence Sensor #43	N	N	N	N	Y
Fan Domain	Fan Domain 0	CPU 1 Fan, CPU 2 Fan	CPU 1 Fan, CPU 2 Fan	CPU 1 Fan, CPU 2 Fan	CPU 1 Fan, CPU 2 Fan	N/A
	Fan Domain 1	System Fan 5	System Fan 5	System Fan 5	System Fan 5	N/A
	Fan Domain 2	System Fan 1	System Fan 1	System Fan 1	System Fan 1	System Fan 1, System Fan2
	Fan Domain 3	System Fan 3	System Fan 3	System Fan 3	System Fan 3	System Fan 3, System Fan 4
Hot-plug Fan Support		N	N	N	N	Y
Fan Redundancy Support		N	N	N	N	Y
Hot-Swap HDD Backplane (HSC) Availability		Y	Y	Y	Y	Y
Power Unit Redundancy Support (PMBus-compliant Power Supply Support)		N	Y	N	Y	Y

Appendix E: 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, you can use the Diagnostic LEDs to identify the last POST process executed.

Each POST code is represented by 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 LED's #4, #5, #6, and #7. The lower nibble bits are represented by Diagnostics LED's #0, #1, #2, and #3. If the bit is set in the upper and lower nibbles, the corresponding LED lights up. If the bit is clear, the corresponding LED is off.

Diagnostic LED #7 is labeled "MSB" (Most Significant Bit), and Diagnostic LED #0 is labeled "LSB" (Least Significant Bit).



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)

Figure 63. Diagnostic LED Placement Diagram

In the following example, the BIOS sends a value of EDh to the diagnostic LED decoder. The LED's are decoded as follows:

Table 84. POST Progress Code LED Example

LED's	Upper Nibble LED's				Lower Nibble LED's			
	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	ON	ON	ON	ON	ON	OFF	ON
Results	1	1	1	0	1	1	0	1
	Eh				Dh			

- Upper nibble bits = 1110b = Eh; Lower nibble bits = 1101b = Dh; the two are concatenated as EDh. Find the meaning of POST Code EDh in below table – Memory Population Error: RDIMMs and UDIMMs cannot be mixed in the system.

Table 85. POST Codes and Messages

Progress Code	Progress Code Definition
Multi-use Code This POST Code is used in different contexts	
0xF2	Seen at the start of Memory Reference Code (MRC)
	Start of the very early platform initialization code
	Very late in POST, it is the signal that the OS has switched to virtual memory mode
Memory Error Codes (Accompanied by a beep code) These codes are used in early POST by Memory Reference Code. Later in POST these same codes are used for other Progress Codes. These progress codes are subject to change as per Memory Reference Code	
0xE8	No Usable Memory Error: No memory in the system, or SPD bad so no memory could be detected, or all memory failed Hardware BIST. System is halted.
0xEB	Memory Test Error: One or memory DIMMs/Channels failed Hardware BIST, but usable memory remains. System continues POST.
0xED	Population Error: RDIMMs and UDIMMs cannot be mixed in the system.
0xEE	Mismatch Error: more than 2 Quad Ranked DIMMS in a channel.
Host Processor	
0x04	Early processor initialization where system BSP is selected
0x10	Power-on initialization of the host processor (Boot Strap Processor)
0x11	Host processor cache initialization (including AP)
0x12	Starting application processor initialization
0x13	SMM initialization
Chipset	
0x21	Initializing a chipset component
Memory	
0x22	Reading configuration data from memory (SPD on DIMM)
0x23	Detecting presence of memory
0x24	Programming timing parameters in the memory controller
0x25	Configuring memory parameters in the memory controller
0x26	Optimizing memory controller settings
0x27	Initializing memory, such as ECC init
0x28	Testing memory
PCI Bus	
0x50	Enumerating PCI buses
0x51	Allocating resources to PCI buses
0x52	Hot-plug PCI controller initialization
0x53-0x57	Reserved for PCI Bus

Progress Code	Progress Code Definition
USB	
0x58	Resetting USB bus
0x59	Reserved for USB devices
ATA/ATAPI/SATA	
0x5A	Resetting SATA bus and all devices
0x5B	Reserved for ATA
SMBUS	
0x5C	Resetting SMBUS
0x5D	Reserved for SMBUS
Local Console	
0x70	Resetting the video controller (VGA)
0x71	Disabling the video controller (VGA)
0x72	Enabling the video controller (VGA)
Remote Console	
0x78	Resetting the console controller
0x79	Disabling the console controller
0x7A	Enabling the console controller
Keyboard (only USB)	
0x90	Resetting the keyboard
0x91	Disabling the keyboard
0x92	Detecting the presence of the keyboard
0x93	Enabling the keyboard
0x94	Clearing keyboard input buffer
0x95	Instructing keyboard controller to run Self Test (PS/2 only)
Mouse (only USB)	
0x98	Resetting the mouse
0x99	Detecting the mouse
0x9A	Detecting the presence of mouse
0x9B	Enabling the mouse
Fixed Media	
0xB0	Resetting fixed media device
0xB1	Disabling fixed media device
0xB2	Detecting the presence of a fixed media device (hard drive detection, etc.)
0xB3	Enabling/configuring a fixed media device
Removable Media	

Progress Code	Progress Code Definition
0xB8	Resetting the removable media device
0xB9	Disabling the removable media device
0xBA	Detecting the presence of a removable media device (CDROM detection, etc.)
0xBC	Enabling/configuring a removable media device
Boot Device Selection	
0xDy	Trying boot selection y (where y = 0 to F)
Pre-EFI Initialization (PEI) Core (not accompanied by a beep code)	
0xE0	Started dispatching early initialization modules (PEIM)
0xE2	Initial memory found, configured, and installed correctly
0xE1,0xE3	Reserved for initialization module use (PEIM)
Driver eXecution Environment (DXE) Core (not accompanied by a beep code)	
0xE4	Entered EFI driver execution phase (DXE)
0xE5	Started dispatching drivers
0xE6	Started connecting drivers
DXE Drivers (not accompanied by a beep code)	
0xE7	Waiting for user input
0xE8	Checking password
0xE9	Entering the BIOS Setup
0xEA	Flash Update
0xEE	Calling Int 19. One beep unless silent boot is enabled.
0xEF	Unrecoverable Boot failure
Runtime Phase/EFI Operating System Boot	
0xF4	Entering the sleep state
0xF5	Exiting the sleep state
0xF8	Operating system has requested EFI to close boot services ExitBootServices ( ) has been called
0xF9	Operating system has switched to virtual address mode SetVirtualAddressMap ( ) has been called
0xFA	Operating system has requested the system to reset ResetSystem () has been called
Pre-EFI Initialization Module (PEIM)/Recovery	
0x30	Crisis recovery has been initiated because of a user request
0x31	Crisis recovery has been initiated by software (corrupt flash)
0x34	Loading crisis recovery capsule
0x35	Handing off control to the crisis recovery capsule
0x3F	Unable to complete crisis recovery

Appendix F: POST Error Messages and Handling

Whenever possible, the BIOS outputs the current boot progress codes on the video screen. Progress codes are 32-bit quantities plus optional data. The 32-bit numbers include class, subclass, and operation information. The class and subclass fields point to the type of hardware being initialized. The operation field represents the specific initialization activity. Based on the data bit availability to display progress codes, you can customize a progress code to fit the data width. The higher the data bit, the higher the granularity of information that can be sent on the progress port. The system BIOS or option ROMs may report progress codes.

The Response section in the following table is divided into three types:

- **No Pause:** The message is displayed on the screen or on the Error Manager screen. 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.
- **Pause:** The 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 will halt and then after the next reset/reboot, it displays the error code in the Error Manager screen.
- **Halt:** 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.

  After entering the BIOS setup, the error message displays 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 must replace the faulty part and restart the system.

Table 86. POST Error Messages and Handling

Error Code	Error Message	Response
0012	CMOS date/time not set	Pause
0048	Password check failed	Pause
0108	Keyboard component encountered a locked error.	No Pause
0109	Keyboard component encountered a stuck key error.	No Pause
0113	Fixed Media The SAS RAID firmware can not run properly. The user should attempt to reflash the firmware.	Pause
0140	PCI component encountered a PERR error.	Pause
0141	PCI resource conflict	Pause
0146	PCI out of resources error	Pause
0192	Processor 0x cache size mismatch detected.	Halt
0193	Processor 0x stepping mismatch.	No Pause
0194	Processor 0x family mismatch detected.	Halt
0195	Processor 0x Intel® QPI speed mismatch.	Pause
0196	Processor 0x model mismatch.	Halt
0197	Processor 0x speeds mismatched.	Halt
0198	Processor 0x family is not supported.	Halt
019F	Processor and chipset stepping configuration is unsupported.	Pause
5220	CMOS/NVRAM Configuration Cleared	Pause
5221	Passwords cleared by jumper	Pause
5224	Password clear Jumper is Set.	Pause
8160	Processor 01 unable to apply microcode update	Pause
8161	Processor 02 unable to apply microcode update	Pause
8180	Processor 0x microcode update not found.	No Pause
8190	Watchdog timer failed on last boot	Pause
8198	OS boot watchdog timer failure.	Pause
8300	Baseboard management controller failed self-test	Pause
84F2	Baseboard management controller failed to respond	Pause
84F3	Baseboard management controller in update mode	Pause
84F4	Sensor data record empty	Pause
84FF	System event log full	No Pause
8500	Memory component could not be configured in the selected RAS mode.	Pause
8520	DIMM_A1 failed Self Test (BIST).	Pause
8521	DIMM_A2 failed Self Test (BIST).	Pause
8522	DIMM_B1 failed Self Test (BIST).	Pause
8523	DIMM_B2 failed Self Test (BIST).	Pause
8524	DIMM_C1 failed Self Test (BIST).	Pause
8525	DIMM_C2 failed Self Test (BIST).	Pause
8526	DIMM_D1 failed Self Test (BIST).	Pause
8527	DIMM_D2 failed Self Test (BIST).	Pause
8528	DIMM_E1 failed Self Test (BIST).	Pause
8529	DIMM_E2 failed Self Test (BIST).	Pause
852A	DIMM_F1 failed Self Test (BIST).	Pause
852B	DIMM_F2 failed Self Test (BIST).	Pause
8540	DIMM_A1 Disabled.	Pause
8541	DIMM_A2 Disabled.	Pause

Error Code	Error Message	Response
8542	DIMM_B1 Disabled.	Pause
8543	DIMM_B2 Disabled.	Pause
8544	DIMM_C1 Disabled.	Pause
8545	DIMM_C2 Disabled.	Pause
8546	DIMM_D1 Disabled.	Pause
8547	DIMM_D2 Disabled.	Pause
8548	DIMM_E1 Disabled.	Pause
8549	DIMM_E2 Disabled.	Pause
854A	DIMM_F1 Disabled.	Pause
854B	DIMM_F2 Disabled.	Pause
8560	DIMM_A1 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8561	DIMM_A2 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8562	DIMM_B1 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8563	DIMM_B2 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8564	DIMM_C1 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8565	DIMM_C2 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8566	DIMM_D1 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8567	DIMM_D2 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8568	DIMM_E1 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8569	DIMM_E2 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
856A	DIMM_F1 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
856B	DIMM_F2 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
85A0	DIMM_A1 Uncorrectable ECC error encountered.	Pause
85A1	DIMM_A2 Uncorrectable ECC error encountered.	Pause
85A2	DIMM_B1 Uncorrectable ECC error encountered.	Pause
85A3	DIMM_B2 Uncorrectable ECC error encountered.	Pause
85A4	DIMM_C1 Uncorrectable ECC error encountered.	Pause
85A5	DIMM_C2 Uncorrectable ECC error encountered.	Pause
85A6	DIMM_D1 Uncorrectable ECC error encountered.	Pause
85A7	DIMM_D2 Uncorrectable ECC error encountered.	Pause
85A8	DIMM_E1 Uncorrectable ECC error encountered.	Pause
85A9	DIMM_E2 Uncorrectable ECC error encountered.	Pause
85AA	DIMM_F1 Uncorrectable ECC error encountered.	Pause
85AB	DIMM_F2 Uncorrectable ECC error encountered.	Pause
8604	Chipset Reclaim of non critical variables complete.	No Pause
9000	Unspecified processor component has encountered a non specific error.	Pause
9223	Keyboard component was not detected.	No Pause
9226	Keyboard component encountered a controller error.	No Pause
9243	Mouse component was not detected.	No Pause
9246	Mouse component encountered a controller error.	No Pause
9266	Local Console component encountered a controller error.	No Pause
9268	Local Console component encountered an output error.	No Pause
9269	Local Console component encountered a resource conflict error.	No Pause
9286	Remote Console component encountered a controller error.	No Pause
9287	Remote Console component encountered an input error.	No Pause
9288	Remote Console component encountered an output error.	No Pause

Error Code	Error Message	Response
92A3	Serial port component was not detected	Pause
92A9	Serial port component encountered a resource conflict error	Pause
92C6	Serial Port controller error	No Pause
92C7	Serial Port component encountered an input error.	No Pause
92C8	Serial Port component encountered an output error.	No Pause
94C6	LPC component encountered a controller error.	No Pause
94C9	LPC component encountered a resource conflict error.	Pause
9506	ATA/ATPI component encountered a controller error.	No Pause
95A6	PCI component encountered a controller error.	No Pause
95A7	PCI component encountered a read error.	No Pause
95A8	PCI component encountered a write error.	No Pause
9609	Unspecified software component encountered a start error.	No Pause
9641	PEI Core component encountered a load error.	No Pause
9667	PEI module component encountered a illegal software state error.	Halt
9687	DXE core component encountered a illegal software state error.	Halt
96A7	DXE boot services driver component encountered a illegal software state error.	Halt
96AB	DXE boot services driver component encountered invalid configuration.	No Pause
96E7	SMM driver component encountered a illegal software state error.	Halt
0xA000	TPM device not detected.	No Pause
0xA001	TPM device missing or not responding.	No Pause
0xA002	TPM device failure.	No Pause
0xA003	TPM device failed self test.	No Pause
0xA022	Processor component encountered a mismatch error.	Pause
0xA027	Processor component encountered a low voltage error.	No Pause
0xA028	Processor component encountered a high voltage error.	No Pause
0xA421	PCI component encountered a SERR error.	Halt
0xA500	ATA/ATPI ATA bus SMART not supported.	No Pause
0xA501	ATA/ATPI ATA SMART is disabled.	No Pause
0xA5A0	PCI Express component encountered a PERR error.	No Pause
0xA5A1	PCI Express component encountered a SERR error.	Halt
0xA5A4	PCI Express IBIST error.	Pause
0xA6A0	DXE boot services driver Not enough memory available to shadow a legacy option ROM.	No Pause
0xB6A3	DXE boot services driver Unrecognized.	Pause

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 of error conditions. The beep code is followed by a user-visible code on the POST Progress LED's.

Table 87. POST Error Beep Codes

Beeps	Error Message	POST Progress Code	Description
3	Memory error	Multiple	System halted because a fatal error related to the memory was detected.

The 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. Each digit in the code is represented by a sequence of beeps whose count is equal to the digit.

Table 88. BMC Beep Codes

Code	Reason for Beep	Associated Sensors
1-5-2-1	CPU: Empty slot/Population error	CPU sockets are populated incorrectly – CPU1 must be populated before CPU2.
1-5-4-2	Power fault: DC power 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.

Appendix G: Installation Guidelines

1. Drivers for Sun Solaris* 10 U5 (05/08)

Device	Description
Chipset	No driver required under Sun Solaris*
Enhanced SATA mode (Onboard SATA)	No driver required under Sun Solaris*
AHCI (Onboard SATA)	No driver required under Sun Solaris*
Onboard NIC (Intel® 82575EB)	No driver required under Sun Solaris*
AXX4SASMOD (Native SAS pass through mode)	No driver required under Sun Solaris*
AXXROMBSASMR	Driver is available from: http://support.intel.com/support/motherboards/server/S5520HC/
ESRTII (Onboard SATA, AXX4SASMOD)	Not currently supported under Sun Solaris*
Onboard Video (ServerEngines*)	No driver required under Sun Solaris*
Intel® Hot Swap Hard Drive back plane	No driver required under Sun Solaris*

2. Sun Solaris* 10 U5 (05/08) hangs during early boot when EHCI-2 is enabled

Description: Sun Solaris* 10 U5 may hang during early boot in the Intel® Server Board S5520HC or S5500HCV when USB 2.0 is Enabled

Guideline: Disable “USB 2.0 Controller” option in BIOS Setup Menu, or follow the instructions listed at the following website in order to accomplish this

http://bugs.opensolaris.org/view_bug.do?bug_id=6681221

3. Sun Solaris* 10 U5 (05/08) may fail to boot into graphics display

Description: Sun Solaris* 10 U5 may fail to boot into graphics display with Intel® Server Board S5520HC or Intel® Server Board S5500HCV onboard video controller

Guideline: Edit the script /usr/bin/X11/Xserver and modify arguments as following in order to accomplish graphics display.

SERVERARGS=”-depth 16 –fbbpp 16”

4. System may experience high power consumption under Microsoft Windows* Server 2003 when the processor is idle

Description: Intel® Server Board S5520HC or Intel® Server Board S5500HCV based system may experience high power consumption under Microsoft Windows* Server 2003 when the processor is idle and there is a discontinuity in the C-states

Guideline: Follow the instructions listed at the following website to apply the hot fix only to systems that are experiencing this problem.

http://support.microsoft.com/kb/941838

5. When EFI Shell is selected as the first device on the BIOS boot option list, some RAID adapters may not enter their configuration screen before the server board boots into EFI Shell.

Description In an Intel® Server Board S5520HC or S5500HCV based system with EFI shell as first boot device, after users press hot keys to enter RAID adapter configuration screen that hooks option ROM on INT 19h, the system may boot in to EFI shell instead.

Guideline Type 'exit' and execute under the EFI shell, the RAID adapter configuration screen will show up if configuration screen hot keys were pressed during POST.

See 32MB video memory of onboard video controller after install onboard video driver

Description After install driver of Intel® Server Boards S5520HC, S5500HCV and S5520HCT onboard video controller, the video driver will report 32MB video memory instead of 8MB

Guideline The memory reported by onboard video driver is 'attached memory', which is accessed by the video controller for internal operations. The graphic memory size for display function is still 8MB

Glossary

Term	Definition
ACPI	Advanced Configuration and Power Interface
AHCI	Advanced Host Controller Interface
AMT	Active Management Technology
AP	Application Processor
APIC	Advanced Programmable Interrupt Control
ARP	Address Resolution Protocol
ASIC	Application Specific Integrated Circuit
ATS	Address Translation Technology
BBS	BIOS Boot Specification
BEV	Boot Entry Vector
BIOS	Basic Input/Output System
BIST	Built-in Self Test
BMC	Baseboard Management Controller
bpp	Bits per pixel
bps	bit per second
BSP	Boot Strap Processor
Byte	8-bit quantity
CL	Controller Link
CLTT	Closed-Loop Thermal Throttling
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.
DCA	Direct Cache Access
DDR3	Double Data Rate 3
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual in-line memory module
DMA	Direct Memory Access
DPC	Direct Platform Control
DXE	Driver eXecution Environment
ECC	Error Correction Code
EEPROM	Electrically Erasable Programmable Read-Only Memory
EFUP	Environment Friendly Usage Period
EHCI	Enhanced Host Controller Interface
EIST	Enhanced Intel SpeedStep® Technology
EMC	Electromagnetic Compatibility
EMP	Emergency Management Port
EPS	External Product Specification
ESI	Enterprise South Bridge Interface
EVRD	Enterprise Voltage Regulator-Down
FMB	Flexible Mother Board
FRB	Fault Resilient Boot
FRU	Field Replaceable Unit
FW	Firmware
FWH	Firmware Hub
GB	1024 MB

Term	Definition
GPA	Guest Physical Address
GPIO	General Purpose I/O
HPA	Host Physical Address
HSC	Hot-Swap Controller
HT	Hyper-Threading
Hz	Hertz (1 cycle/second)
I2C	Inter-Integrated Circuit Bus
IA	Intel® Architecture
ICH	I/O Controller Hub
ILM	Independent Loading Mechanism
IMC	Integrated Memory Controller
INTR	Interrupt
IOH	I/O HUB
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
IRQ	Interrupt request
ITE	Information Technology Equipment
JBOD	Just Bunch of Disks
JRE	Java Runtime Environment
KB	1024 bytes
KVM	Keyboard, Video, and Mouse
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Authentication Protocol
LED	Light Emitting Diode
LPC	Low-Pin Count
LSB	Least Significant Bit
LUN	Logical Unit Number
MAC	Media Access Control
MB	1024 KB
ME	Manageability Engine
MMU	Memory Management Unit
MRC	Memory Reference Code
ms	Milliseconds
MSB	Most Significant Bit
MTBF	Mean Time Between Failures
Mux	Multiplexer
NIC	Network Interface Controller
Nm	Nanometer
NMI	Non-maskable Interrupt
NUMA	Non-Uniform Memory Access
NVSRAM	Non-volatile Static Random Access Memory
OEM	Original Equipment Manufacturer
Ohm	Unit of electrical resistance
OLTT	Open-Loop Thermal Throttling
PAE	Physical Address Extension

Term	Definition
PCB	Print Circuit Board
PCI	Peripheral Component Interconnect
PECI	Platform Environment Control Interface
PEF	Platform Event Filtering
PEP	Platform Event Paging
PMBus	Power Management Bus
PMI	Platform Management Interrupt
POST	Power-on Self Test
PWM	Pulse-Width Modulation
QPI	QuickPath Interconnect
RAID	Redundant Array of Independent Disks
RAS	Reliability, Availability, and Serviceability
RASUM	Reliability, Availability, Serviceability, Usability, and Manageability
RDIMM	Registered Dual In-Line Memory Module
RISC	Reduced Instruction Set Computing
RMII	Reduced Media Independent Interface
ROM	Read Only Memory
RTC	Real-Time Clock (Component of ICH peripheral chip on the server board)
SAS	Serial Attached SCSI
SATA	Serial ATA
SDR	Sensor Data Record
SEEPROM	Serial Electrically Erasable Programmable Read-Only Memory
SEL	System Event Log
SES	SCSI Enclosure Services
SGPIO	Serial General Purpose Input/Output
SMBus	System Management Bus
SMI	Server Management Interrupt (SMI is the highest priority nonmaskable interrupt)
SMS	Server Management Software
SNMP	Simple Network Management Protocol
SOL	Serial Over LAN
SPD	Serial Presence Detect
SPI	Serial Peripheral Interface
SPS	Server Platform Service
SSD	Solid State Drive
TBD	To Be Determined
TDP	Thermal Design Power
TIM	Thermal Interface Material
TPS	Technical Product Specification
UART	Universal Asynchronous Receiver/Transmitter
UDIMM	Unbuffered Dual In-Line Memory Module
UDP	User Datagram Protocol
UHCI	Universal Host Controller Interface
URS	Unified Retention System
USB	Universal Serial Bus
UTC	Universal time coordinate
VGA	Video Graphic Array

Term	Definition
VID	Voltage Identification
VLSI	Very-large-scale integration
VRD	Voltage Regulator Down
VT	Virtualization Technology
VT-d	Virtualization Technology for Directed I/O
Word	16-bit quantity
WS-MAN	Web Service for Management
XD bit	Execute Disable Bit

Reference Documents

See the following documents for additional information:

Intel® Server Boards S5520HC and S5500HCV Specification Update

Mouser Electronics

Authorized Distributor

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

Intel:

S5520HCR BB5520HCR BB5500HCV S5520HCT S5500HCVR BB5500HCVR

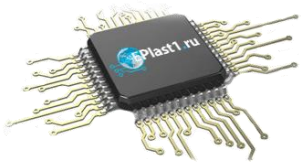
Компания «ЭлектроПласт» предлагает заключение долгосрочных отношений при поставках импортных электронных компонентов на взаимовыгодных условиях!

Наши преимущества:

- Оперативные поставки широкого спектра электронных компонентов отечественного и импортного производства напрямую от производителей и с крупнейших мировых складов;
- Поставка более 17-ти миллионов наименований электронных компонентов;
- Поставка сложных, дефицитных, либо снятых с производства позиций;
- Оперативные сроки поставки под заказ (от 5 рабочих дней);
- Экспресс доставка в любую точку России;
- Техническая поддержка проекта, помощь в подборе аналогов, поставка прототипов;
- Система менеджмента качества сертифицирована по Международному стандарту ISO 9001;
- Лицензия ФСБ на осуществление работ с использованием сведений, составляющих государственную тайну;
- Поставка специализированных компонентов (Xilinx, Altera, Analog Devices, Intersil, Interpoint, Microsemi, Aeroflex, Peregrine, Syfer, Eurofarad, Texas Instrument, Miteq, Cobham, E2V, MA-COM, Hittite, Mini-Circuits,General Dynamics и др.);

Помимо этого, одним из направлений компании «ЭлектроПласт» является направление «Источники питания». Мы предлагаем Вам помощь Конструкторского отдела:

- Подбор оптимального решения, техническое обоснование при выборе компонента;
- Подбор аналогов;
- Консультации по применению компонента;
- Поставка образцов и прототипов;
- Техническая поддержка проекта;
- Защита от снятия компонента с производства.



Как с нами связаться

Телефон: 8 (812) 309 58 32 (многоканальный)
Факс: 8 (812) 320-02-42
Электронная почта: org@eplast1.ru
Адрес: 198099, г. Санкт-Петербург, ул. Калинина, дом 2, корпус 4, литера А.