Intel® Server Board S5520UR and S5520URT

Technical Product Specification

Intel order number E44031-012

Revision 1.9

May, 2011

Enterprise Platforms and Services Division - Marketing

Revision History

Date	Revision Number	Modifications
March 2009	1.0	Initial Release.
October 2009	1.1	Updated section 3.2 - Memory Subsystem.
January 2010	1.2	▪ Updated section 2.1 and added Security Feature for S5520URT. ▪ Updated section 2.2.3 - NIC Connector. ▪ Added section 3.9 Trusted Platform Module.
March 2010	1.3	▪ Updated section 2.1 - Intel® Server Board S5520UR, S5520URT Feature Set. ▪ Updated section 3.1 - Intel® Xeon® Processor 5600 Series. ▪ Updated section 3.2.4 - Memory RAS. ▪ Updated section 3.2.5 - Memory Upgrade Rules. ▪ Updated section 3.2.1 - Supported memory.
Arpil 2010	1.4	▪ Updated section 2.2.1 - Server Board Connector and Component Layout. ▪ Removed section 3.6.2 - Serial Port. ▪ Removed CCC/WEEE.
May 2010	1.5	Added section 3.9.3 - Intel® Trusted Execution Technology (Intel® TXT).
July 2010	1.6	▪ Updated section 3.7 - Video Support. ▪ Updated section 3.3.2 - DDR3 Memory Configuration.
December 2010	1.7	▪ Updated section 2.1 - Intel® Server Board S5520UR, S5520URT Feature Set. ▪ Updated section 2 - Overview.
	1.8	Updated section 2.1 - Intel® Server Board S5520UR , S5520URT Feature Set.
May 2011	1.9	▪ Added section 5 – BIOS Setup Utility. ▪ Updated section 3.5 – I/O Module. ▪ Updated section 3.8 - Network Interface Controller (NIC).

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 Board S5520UR and S5520URT may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel Corporation server boards 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 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 is intentionally left blank.>

1. Introduction

This Technical Product Specification (TPS) provides board-specific information detailing the features, functionality, and high-level architecture of the Intel® Server Board S5520UR, S5520URT.

In addition, design-level information for specific subsystems can be obtained by ordering the External Product Specifications (EPS) or External Design Specifications (EDS) for a given subsystem. EPS and EDS documents are not publicly available and must be ordered 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 – Connector/Header Locations and Pin-outs
- Chapter 6 – Configuration Jumpers
- Chapter 7 – Intel® Light-Guided Diagnostics
- Chapter 8 – Design and Environmental Specifications
- Chapter 9 – Regulatory and Certification Information
- Appendix A – Integration and Usage Tips
- Appendix B – Integrated BMC Sensor Tables
- Appendix C – Management Engine Generated SEL Event Messages
- Appendix D – POST Code Diagnostic LED Decoder
- Appendix E – POST Code Errors
- Appendix F – Supported Intel® Server Chassis
- Glossary
- Reference Documents

1.2 Server Board Use Disclaimer

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 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 their published operating or non-operating limits.

2. Overview

The Intel® Server Board S5520UR is a monolithic printed circuit board with features that are designed to support the rack server markets.

2.1 Intel® Server Board S5520UR, S5520URT Feature Set

Table 1. Intel® Server Board S5520UR, S5520URT Feature Set

Feature	Description
Processors	Support ▪ 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 ▪ Enterprise Voltage Regulator-Down (EVRD) 11.1
Memory	Support for 800/1066/1333 MT/s ECC registered (RDIMM) or unbuffered (UDIMM) DDR3 memory. 12 DIMMs total across 6 memory channels (3 channels per processor).
Chipset	Intel® 5520 Chipset IOH Intel® 82801Jx I/O Controller Hub (ICH10R)
I/O Control	External connections: ▪ DB-15 Video connector ▪ RJ-45 serial Port A connector ▪ Two RJ-45 Network Interface Connectors for 10/100/1000 Mb ▪ Four USB 2.0 connectors Internal connections: ▪ One USB 2x5 pin header, supporting two USB 2.0 ports ▪ One low-profile USB 2x5 pin header to support low-profile USB solid state drives ▪ One DH-10 Serial Port B header ▪ Six SATA II connectors ▪ Two I/O module Mezzanine connectors for optional I/O Module support ▪ One RMM3 connector to support optional Intel® Remote Management Module 3 ▪ SATA SW RAID 5 Activation Key Connector ▪ One SSI-EEB compliant front panel header ▪ One SSI-EEB compliant 24-pin main power connector ▪ One SSI-compliant 8-pin CPU power connector ▪ One SSI-compliant power supply SMBus connector
System Fan Support	Six 4-pin fan headers supporting 2 processor fans, 2 memory fans, and up to 2 system fans One 26-pin custom system fan header for use in an Intel® Server Chassis
Add-in Adapter Support	One riser slot supporting both full-height and low-profile 1U and 2U PCI Express* riser cards
Video	On-board ServerEngines* LLC Pilot II Controller ▪ Integrated 2D Video Controller ▪ 64 MB DDR2 Memory
Hard Drive	Support for six ICH10R SATA II ports

Feature	Description
LAN	Two 10/100/1000 ports provided by Intel® 82575 PHYs with Intel® I/O Acceleration Technology 2 support.
Security**	Trusted Platform Module
Server Management	On-board 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® Server Management Software 3.1

**The Trusted Platform Module is only availabe in S5520URT.

2.2 Server Board Layout

Figure 1. Intel® Server Board S5520UR

2.2.1 Server Board Connector and Component Layout

The following figure shows the board layout of the server board. Each connector and major component is identified by a number or letter, and a description is given in Table 2.

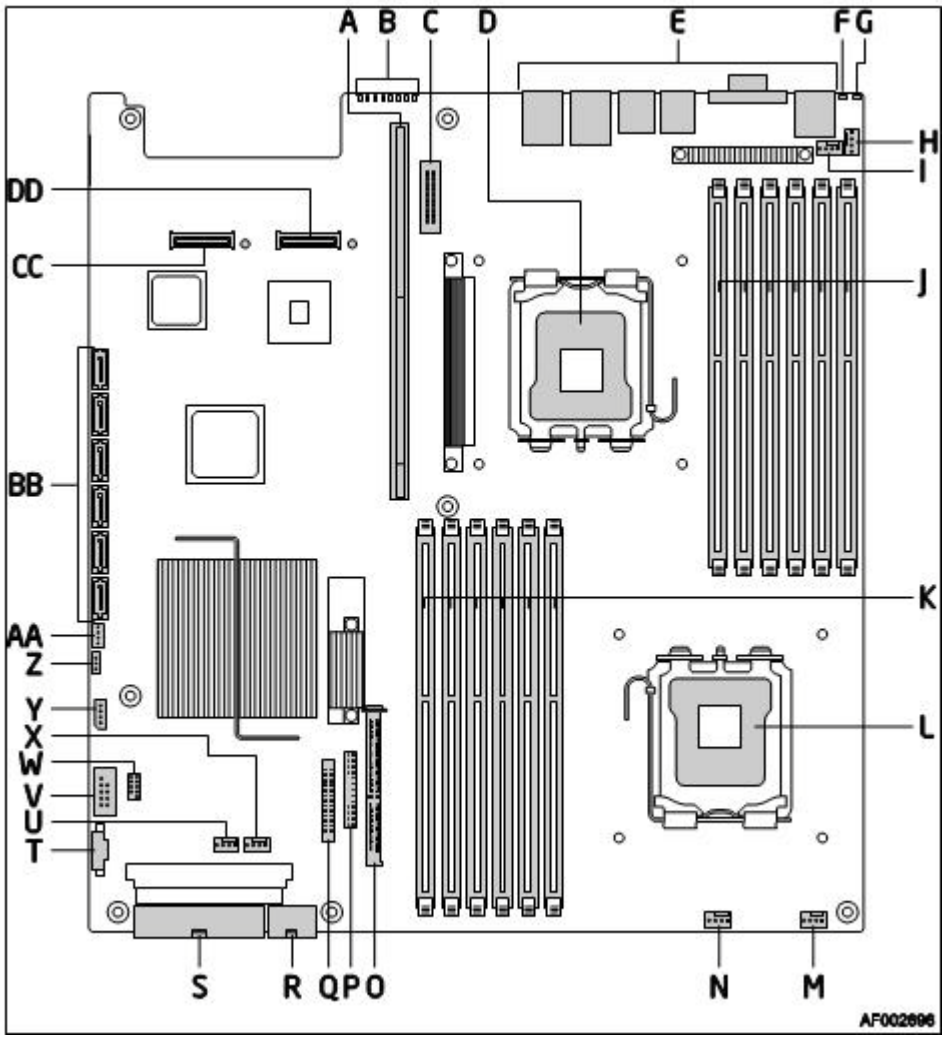


Figure 2. Intel® Server Board S5520UR, S5520URT Layout

Table 2. Major Board Components

	Description		Description
A	280-pin Intel® Adaptive Riser Card Slot	Q	Fan Board Connector (Intel® Server Chassis)
B	POST Code LEDs	R	2x4 Power Connector
C	Intel® RMM3 Header	S	Main Power Connector
D	Processor 1	T	Power Supply SMBus Connector
E	Back Panel I/O	U	Fan Header
F	ID LED	V	USB Header
G	System Status LED	W	Low-profile USB Solid State Driver Header
H	Fan Header	X	Fan Header
I	Fan Header	Y	LCP IPMB Header
J	Processor 1 DIMM Slots	Z	SATA RAID 5 Key Header
K	Processor 2 DIMM Slots	AA	SGPIO Header
L	Processor 2	BB	SATA Connectors
M	Fan Header	CC	I/O Module Mezzanine Connector 2
N	Fan Header	DD	I/O Module Mezzanine Connector 1
O	Bridge Board Connector (Intel® Server Chassis)		
P	Front Panel Connector		

2.2.2 Intel® Server Board S5520UR, S5520URT Mechanical Drawings

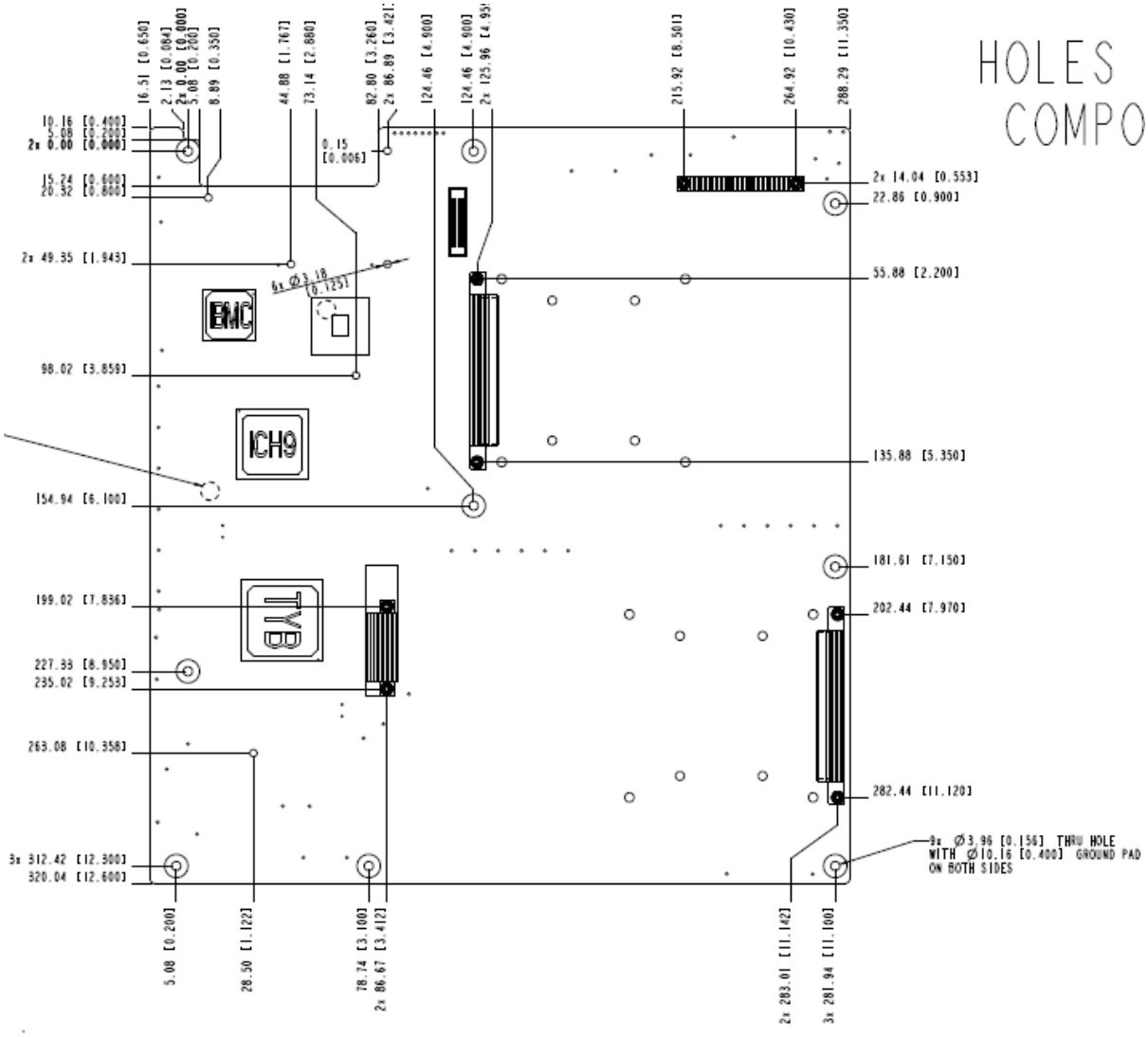


Figure 3. Intel® Server Board S5520UR, S5520URT – Hole and Component Positions (1 of 2)

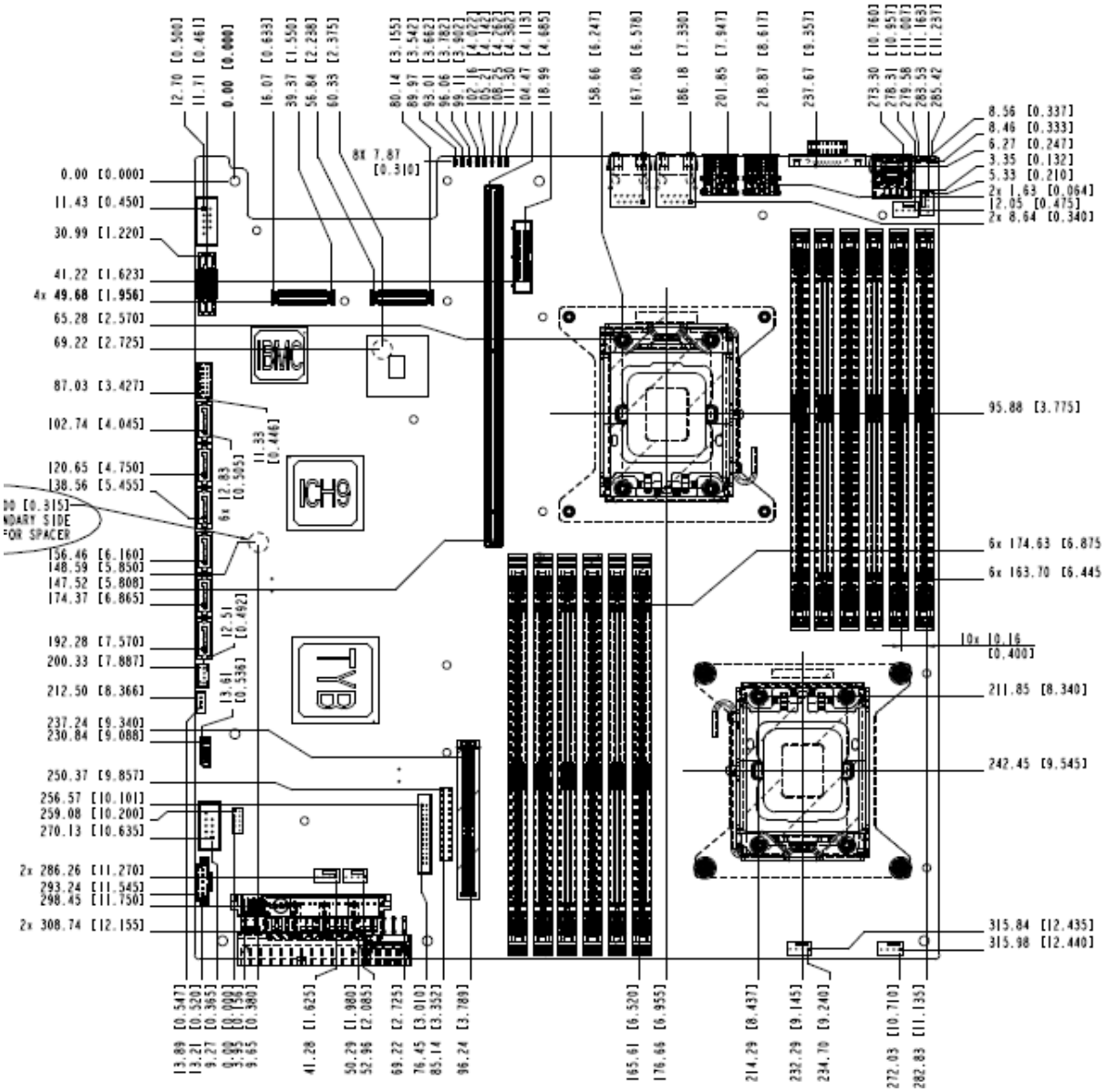


Figure 4. Intel® Server Board S5520UR, S5520URT – Hole and Component Positions (2 of 2)

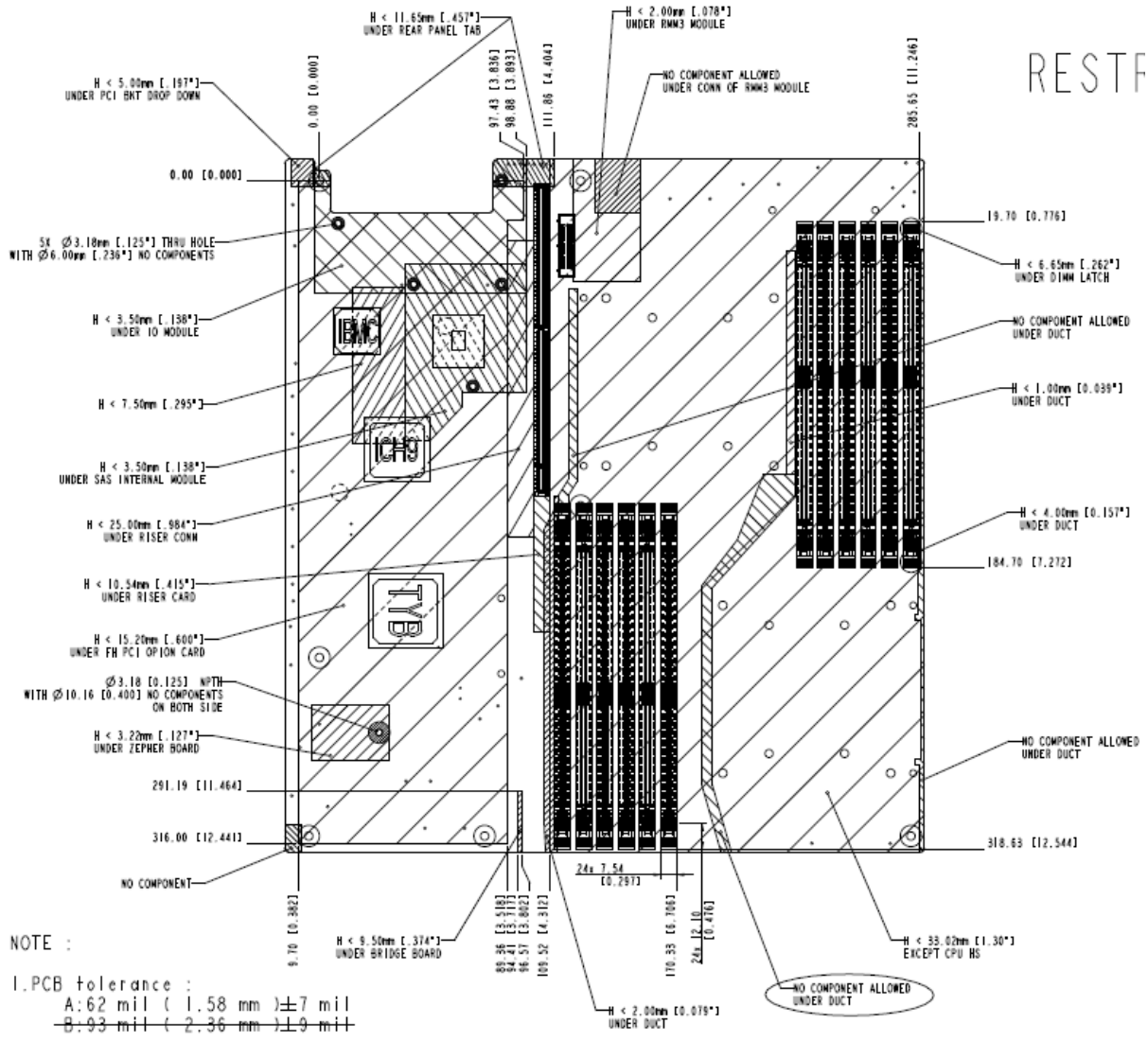


Figure 5. Intel® Server Board S5520UR, S5520URT – Primary Side Keepout Zone (1 of 3)

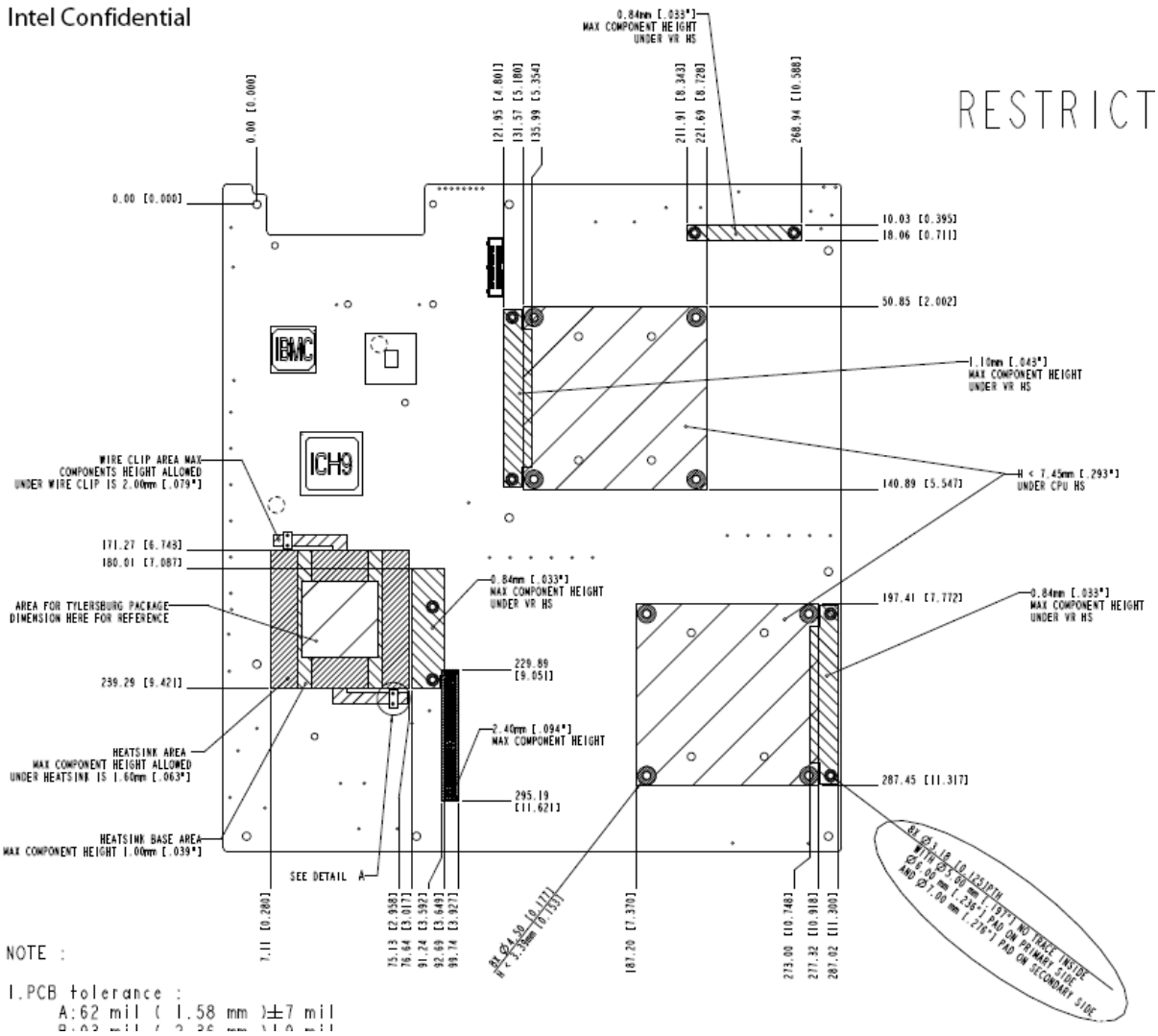


Figure 6. Intel® Server Board S5520UR, S5520URT– Primary Side Keepout Zone (2 of 3)

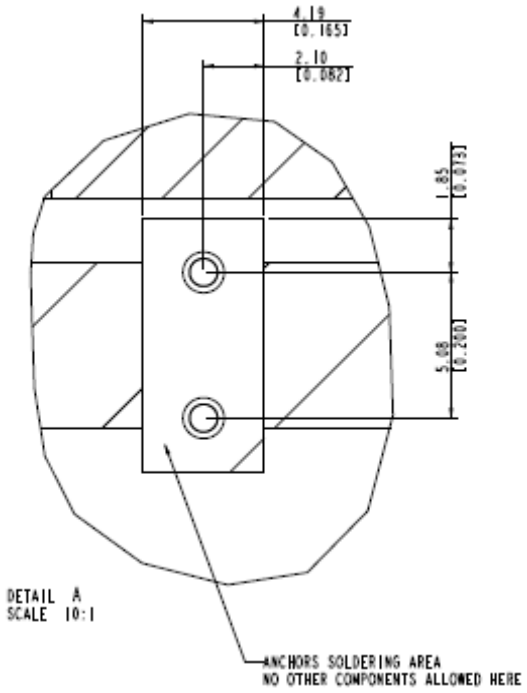


Figure 7. Intel® Server Board S5520UR, S5520URT– Primary Side Keepout Zone (3 of 3)

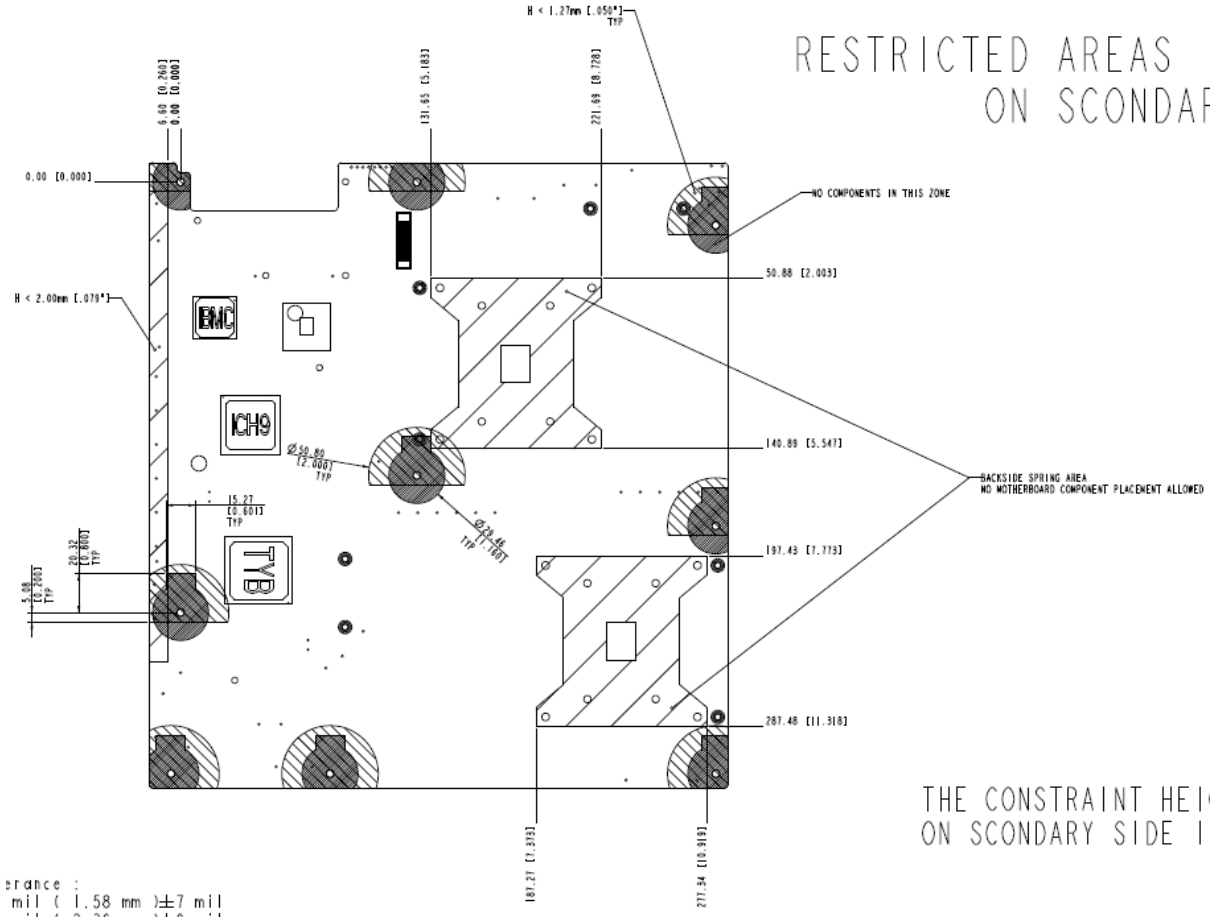
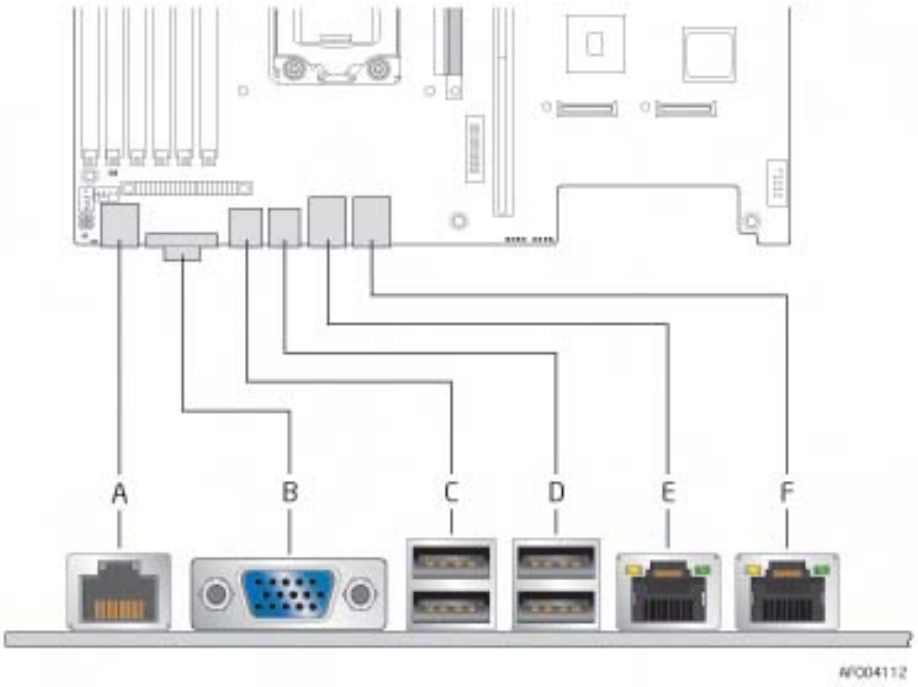


Figure 8. Intel® Server Board S5520UR, S5520URT– Second Side Keepout Zone

2.2.3 Server Board Rear I/O Layout

The following figure shows the layout of the rear I/O components for the server board.



A	Serial Port A	D	Dual USB Port Connector
B	Video	E	NIC Port 1 (1 Gb)
C	Dual USB Port Connector	F	NIC Port 2 (1 Gb)

Figure 9. Intel® Server Board S5520UR, S5520URT Rear I/O Layout

3. Functional Architecture

The architecture and design of the Intel® Server Board S5520UR, S5520URT is based on the Intel® 5520 Chipset I/O Hub (IOH) and ICH10R chipset. The chipset is designed for systems based on the Intel® Xeon® processor in FC-LGA 1366 socket B package with Intel® QuickPath Interconnect (Intel® QPI). The chipset contains two main components:

- Intel® 5520 Chipset IOH, which provides a connection point between various I/O components.
- Intel® QPI, which is the I/O controller hub (ICH10R) for the I/O subsystem. The chipset uses ICH10R for the I/O controller hub.

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

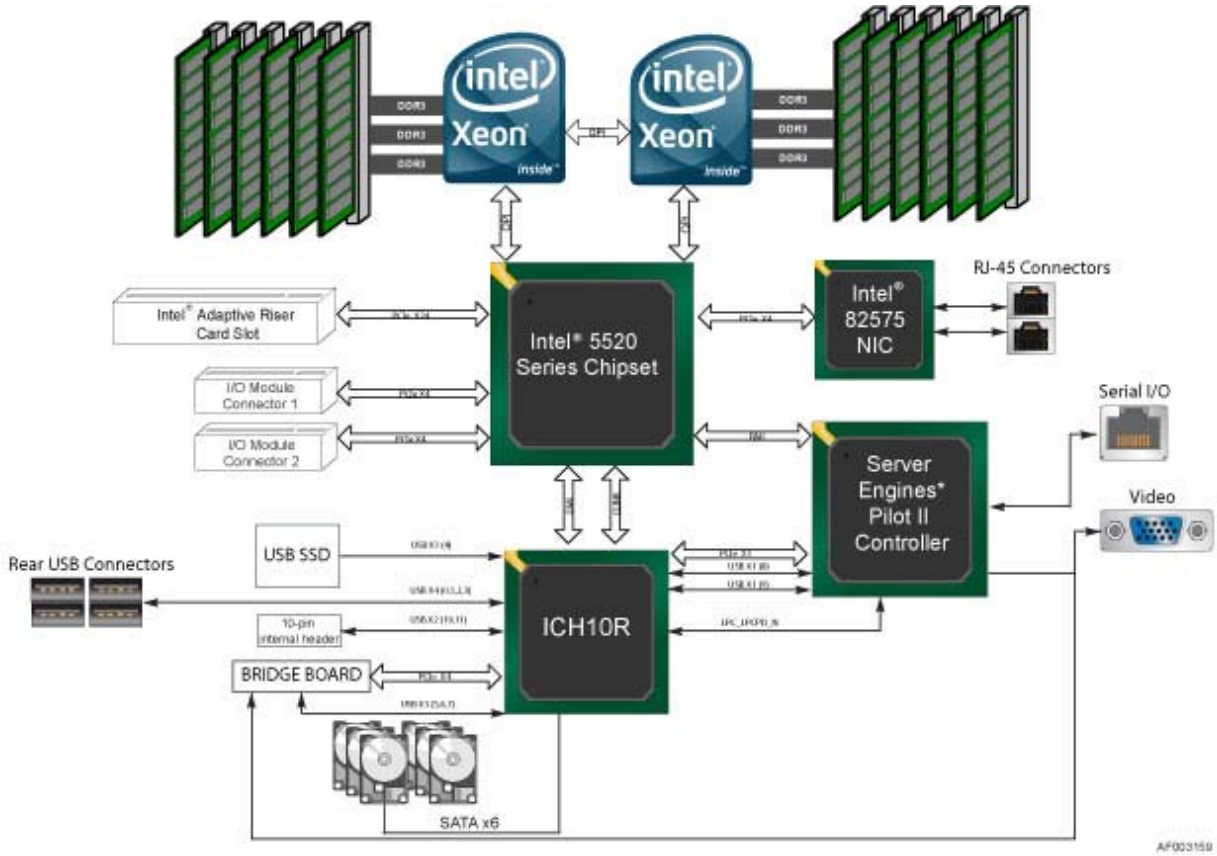


Figure 10. Intel® Server Board S5520UR, S5520URT Functional Block Diagram

3.1 Intel® Xeon® Processor

3.1.1 Processor Support

The Intel® Server Boards S5520UR supports 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://www.intel.com/p/en_US/support/highlights/server/s5520ur. On the **Support** tab, look for **Compatibility** and then **Supported Processor List**.

3.1.1.1 Processor Population Rules

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

When using a single processor configuration, the processor must be installed into the processor socket labeled CPU1. A terminator is not required in the second processor socket when using a single processor configuration.

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

- Both processors must be of the same processor family.
- Both processors must have the same cache size.
- Processors with different speeds can be mixed in a system, given the prior rules are met. If this condition is detected, all processor speeds are set to the lowest common denominator (highest common speed) and an error is reported.
- Processor stepping within a common processor family can be mixed as long as it is listed in the processor specification updates published by Intel Corporation.

The following table describes mixed processor conditions and recommended actions for all Intel® server boards and systems that use the Intel® 5520 Chipset. The errors fall into one of the following two categories:

- **Fatal:** If the system can boot, it goes directly to the error manager, regardless of whether the **Post Error Pause** setup option is enabled or disabled.
- **Major:** If the **Post Error Pause** setup option is enabled, system goes directly to the error manager. Otherwise, the system continues to boot and no prompt is given for the error. The error is logged to the error manager.

Table 3. Mixed Processor Configurations

Error	Severity	System Action
Processor family not identical	Fatal	The BIOS detects the error condition and responds as follows: ▪ Logs the error into the system event log (SEL). ▪ Alerts the Integrated BMC of the configuration error with an IPMI command. ▪ Does not disable the processor. ▪ Displays “0194: Processor family mismatch detected” message in the error manager. ▪ Halts the system.
Processor cache not identical	Fatal	The BIOS detects the error condition and responds as follows: ▪ Logs the error into the SEL. ▪ Alerts the Integrated BMC of the configuration error with an IPMI command. ▪ Does not disable the processor. ▪ Displays “0192: Cache size mismatch detected” message in the error manager. ▪ Halts the system.
Processor frequency (speed) not identical	Major	The BIOS detects the error condition and responds as follows: ▪ Adjusts all processor frequencies to lowest common denominator. ▪ 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 speeds mismatched” message in the error manager. ▪ Halts the system.
Processor microcode missing	Fatal	The BIOS detects the error condition and responds as follows: ▪ Logs the error into the SEL. ▪ Alerts the Integrated BMC of the configuration error with an IPMI command. ▪ Does not disable processor. ▪ Displays “816x: Processor 0x unable to apply microcode update” message in the error manager. ▪ Pauses the system for user intervention.
Processor Intel® QuickPath Interconnect speeds 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 of the configuration error with an IPMI command. ▪ Does not disable the processor. ▪ Displays “0195: Processor Front Side Bus speed mismatch detected” message in the error manager. ▪ Halts the system.

3.1.2 Turbo Mode

The Turbo Mode feature allows extreme edition processors to program thresholds for power/current which can increase platform performance by 10%.

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

3.1.3 Hyperthreading

Most Intel® Xeon® processors support hyper threading. The BIOS detects processors that support this feature and enables the feature during POST.

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

3.1.4 Intel® QuickPath Interconnect

Intel® QPI is a cache-coherent, link-based interconnect specification for processor, chipset, and I/O bridge components. Intel® QPI can be used in a wide variety of desktop, mobile, and server platforms spanning IA-32 and Intel® Itanium® architectures. Intel® QPI also provides support for high-performance I/O transfer between I/O nodes. It allows connection to standard I/O buses such as PCI Express*, PCI-X, PCI (including peer-to-peer communication support), AGP, through appropriate bridges.

Each Intel® QPI link consists of 20 pairs of uni-directional differential lanes for the transmitter and receiver, plus a differential forwarded clock. A full width Intel® QPI link pair consists of 84 signals (20 differential pairs in each direction) plus a forwarded differential clock in each direction. Each Intel® Xeon® Processor 5500 series processor and Intel® Xeon® Processor 5600 series processor supports two Intel® QPI links, one going to the other processor and the other to the Intel® 5520 Chipset IOH.

In the current implementation, Intel® QPI ports are capable of operating at transfer rates of up to 6.4 GT/s. Intel® QPI ports operate at multiple lane widths (full - 20 lanes, half - 10 lanes, quarter - 5 lanes) independently in each direction between a pair of devices communicating via Intel® QPI. The server board supports full width communication only.

3.1.5 Unified Retention System Support

The server board complies with Intel®'s Unified Retention System (URS) and the Unified Backplate Assembly. The server board ships with a made-up assembly of Independent Loading Mechanism (ILM) and Unified Backplate at each processor socket.

The URS retention transfers load to the server board via the unified backplate assembly. The URS spring, captive in the heatsink, provides the necessary compressive load for the thermal interface material. All components of the URS heatsink solution are captive to the heatsink and only require a Philips* screwdriver to attach to the unified backplate assembly. See the following figure for the stacking order of the URS components.

The ILM and unified backplate are removable, allowing for the use of non-Intel® heatsink retention solutions.

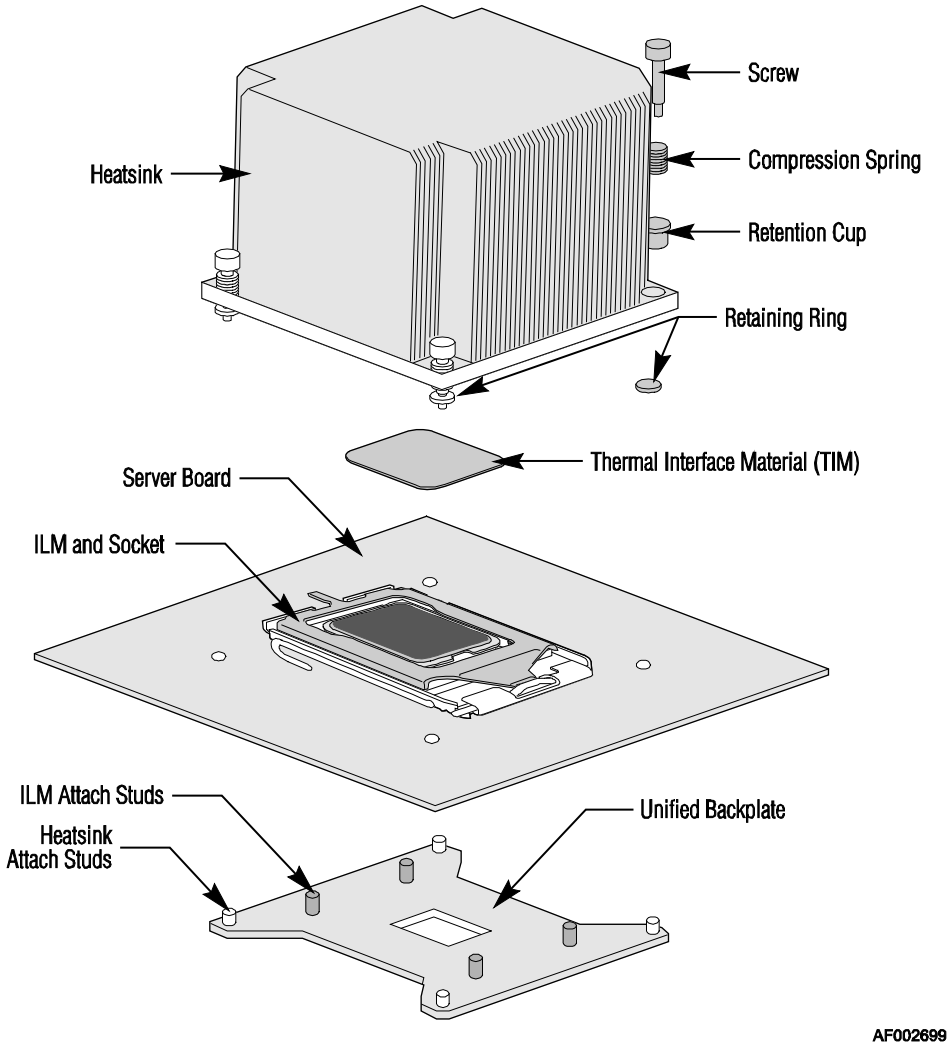


Figure 11. Unified Retention System and Unified Backplate Assembly

3.2 Memory Subsystem

3.2.1 Intel® QuickPath Memory Controller

The Intel® Xeon® Processor 5500 Series and Intel® Xeon® Processor 5600 Series have an integrated memory controller in its package. The Intel® QuickPath Memory Controller supports DDR3 800, DDR3 1066, and DDR3 1333 memory technologies.

The memory controller supports both registered DIMMs (RDIMMs) and unbuffered DIMMs (UDIMMs). The presence of a single non-ECC UDIMM results in the disabling of ECC functionality.

The Channel Independent mode is the only memory RAS mode that supports non-ECC DIMMs.

DIMMs with different timing parameters can be installed on different slots within the same channel. But timings that support the slowest DIMM are applied to all. As a consequence, faster DIMMs are operated at timings supported by the slowest DIMM populated. The same interface frequency is applied to all DIMMs on all channels.

3.2.1.1 Supported Memory

The Intel® Server Board S5520UR, S5520URT supports six DDR3 memory channels (three per processor socket) with two DIMMs per channel, thereby supporting up to 12 DIMMs with dual-processor sockets with a maximum memory capacity of 192 GB.

- The Intel® Xeon® Processor 5500 Series on the Intel® Server Board S5520UR, S5520URT supports up to 12 DDR3 DIMMs with 1.5 V and a maximum of 192 GB memory capacity.
- The Intel® Xeon® Processor 5600 Series on the Intel® Server Board S5520UR, S5520URT supports up to 12 DDR3 DIMMs with 1.5 V or 1.35V and a maximum of 192 GB memory capacity.
- Intel® Server Board S5520UR, S5520URT supports 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 on the Intel® Xeon® Processor 5500 Series
    - 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
- The Intel® Xeon® Processor 5500 Series on the Intel® Server Board S5520UR, S5520URT supports 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

- The Intel® Xeon® Processor 5600 Series on the Intel® Server Board S5520UR, S5520URT supports the following DIMM and DRAM technologies:
  - RDIMMs:
    - Single-, Dual-, and Quad-Rank
    - The Intel® Xeon® Processor 5600 Series support all Intel® Xeon® Processor 5500 Series memory configuration.
    - Any combination of x 4 or x8 RDIMMs, with 1 Gb, 2 Gb or 4Gb DRAM density, is supported.
    - All channels in a system will run at fastest common frequency.
    - If 1.35V and 1.5V DIMMs are mixed, the DIMMs will run at 1.5V

  - UDIMMs:
    - Single- and Dual-Rank
    - The Intel® Xeon® Processor 5600 Series support all Intel® Xeon® Processor 5500 Series memory configuration.
    - Any combination of x 8 or x16 UDIMMs, with 1 Gb, 2 Gb DRAM density, is supported.
    - 2 DIMMs Populated per Channel at 1333 MT/s is only supported on UDIMMs with ECC support.
    - DDR3 1333, DDR3 1066, and DDR3 800
    - If 1.35V and 1.5V DIMMs are mixed, the DIMMs will run at 1.5V
    - The Intel® Xeon® Processor 5600 Series and DDR3L UDIMMs without ECC is not a validated configuration.

3.2.2 Processor Cores, QPI Links and DDR3 Channels Frequency Configuration

The Intel® Xeon® 5500 series processor and Intel® Xeon® 5600 series processor connects to other Intel® Xeon® 5500 series processor and Intel® Xeon® 5600 series processor and Intel® 5520 IOH through the Intel® QPI link interface. The frequencies of the processor cores and the QPI links of Intel® Xeon® 5500 series processor and Intel® Xeon® 5600 series processor are independent from each other. There are no gear-ratio requirements for the Intel® Xeon® Processor 5500 Series and Intel® Xeon® 5600 series processor.

Intel® 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 in the following tables (Tables 3 and 4 and 5) also determine the global common memory system frequency.

Table 4. 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 5. Memory Running Frequency vs. Memory Population for Intel® Xeon® 5500 series processor

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 fastest common frequency of processor IMCs and installed memory: 800 MHz, 1066 MHz, or 1333 MHz
RDIMM	1	Y	Y	N	1N	QR Only	All RDIMMs run at 800 MHz or 1066 MHz when Quad-Rank RDIMM installed in any channel.
RDIMM	2	Y	Y	N	1N	SR or DR	All RDIMMs run at 800 MHz or 1066 MHz when two RDIMMs (Single-Rank or Dual-Rank) installed in the same channel.
RDIMM	2	Y	N	N	1N	QR only	All RDIMMs run at 800 MHz when two RDIMMs (either or both are Quad-Rank RDIMMs) are installed in the same channel.
UDIMM w or w/o ECC	1	Y	Y	Y	1N	SR or DR	All UDIMMs run at fastest common frequency of processor IMCs and installed memory: 800 MHz, 1066 MHz , or 1333 MHz
UDIMM	2	Y	Y	N	2N	SR or DR	All UDIMMs run at 800 MHz or 1066 MHz

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			
w or w/o ECC							when two UDIMMs (Single- or Dual-Rank) are installed in the same channel.

Note:

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

Table 6. Memory Running Frequency vs. Memory Population for Intel® Xeon® 5600 series processor

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 1.5V w/ ECC	1	Y	Y	Y	1N	SR or DR	All RDIMMs run at the fastest common frequency of processor IMCs and installed memory: 800 MHz, 1066 MHz, or 1333 MHz
RDIMM 1.5V w/ ECC	1	Y	Y	N	1N	QR Only	All RDIMMs run at 800 MHz or 1066 MHz when Quad-Rank RDIMM installed in any channel.
RDIMM 1.5V w/ ECC	2	Y	Y	Y	1N	Mixing SR , DR	All RDIMMs run at the fastest common frequency of processor IMCs and installed memory: 800 MHz, 1066 MHz, or 1333 MHz
RDIMM 1.5V w/ ECC	2	Y	N	N	1N	Mixing SR , DR , QR	All RDIMMs run at the fastest common frequency of processor IMCs and installed memory: 800 MHz
RDIMM DDR3L 1.35V w/ ECC	1	Y	Y	Y	1N	SR or DR	All RDIMMs run at the fastest common frequency of processor IMCs and installed memory: 800 MHz, 1066 MHz, or 1333 MHz
RDIMM DDR3L 1.35V w/ ECC	1	Y	N	N	1N	QR Only	All RDIMMs run at the fastest common frequency of processor IMCs and installed memory: 800 MHz
RDIMM DDR3L	2	Y	Y	N	1N	Mixing SR , DR	All RDIMMs run at the fastest common frequency of processor IMCs and

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			
1.35V w/ECC							installed memory: 800 MHz, 1066 MHz
RDIMM DDR3L 1.35V w/ECC	2	Y	N	N	1N	Mixing SR , DR , QR	All RDIMMs run at the fastest common frequency of processor IMCs and installed memory: 800 MHz
UDIMM 1.5V w or w/o ECC	1	Y	Y	Y	1N	SR or DR	All UDIMMs run at the fastest common frequency of processor IMCs and installed memory: 800 MHz, 1066 MHz, or 1333 MHz(2 DIMMs Populated per Channel at 1333 MT/s is only supported on UDIMMs with ECC support)
UDIMM 1.5V w or w/o ECC	2	Y	Y	Y	2N	Mixing SR , DR	All UDIMMs run at the fastest common frequency of processor IMCs and installed memory: 800 MHz, 1066 MHz, or 1333 MHz(2 DIMMs Populated per Channel at 1333 MT/s is only supported on UDIMMs with ECC support)
UDIMM 1.35V w/ECC	1	Y	Y	Y	1N	SR or DR	All UDIMMs run at the fastest common frequency of processor IMCs and installed memory: 800 MHz, 1066 MHz, or 1333 MHz
UDIMM 1.35V w/ECC	2	Y	Y	N	2N	Mixing SR , DR	All UDIMMs run at the fastest common frequency of processor IMCs and installed memory: 800 MHz, 1066 MHz,

Notes:

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

3.2.3 Publishing System Memory

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

The nomenclature for DIMM sockets implemented on the Intel® Server Board S5520UR, S5520URT is detailed in the following table:

Table 7. DIMM Nomenclature

Processor Socket 1						Processor Socket 2					
Channel A		Channel B		Channel C		Channel D		Channel E		Channel F	
A1	A2	B1	B2	C1	C2	D1	D2	E1	E2	F1	F2

3.2.3.1 Memory Subsystem Nomenclature

- DIMMs are organized into physical slots on DDR3 memory channels that belong to processor sockets.
- The memory channels from processor socket 1 are identified as Channel A, B, and C. The memory channels from processor socket 2 are identified as Channel D, E, and F.
- The silk screened DIMM slot identifiers on the board provide information about the channel, and therefore the processor to which they belong. For example, DIMM_A1 is the first slot on Channel A on processor 1; DIMM_D1 is the first DIMM socket on Channel D on processor 2.
- The memory slots associated with a given processor are unavailable if the given processor socket is not populated.
- A processor may be installed without populating the associated memory slots provided a second processor is installed with associated memory. In this case, the memory is shared by the processors. However, the platform suffers performance degradation and latency due to the remote memory.
- Processor sockets are self-contained and autonomous. However, all memory subsystem support (such as Memory RAS, Error Management,) in the BIOS setup are applied commonly across processor sockets.

3.2.4 Memory RAS

3.2.4.1 RAS Features

The server board supports the following memory RAS features:

- Channel Independent Mode
- Channel Mirroring Mode

The memory RAS offered by the Intel® Xeon® Processor 5500 Series and Intel® Xeon® Processor 5600 Series is done at channel level, i.e., during mirroring, channel B mirrors channel A. All DIMM matching requirements are on a slot to slot basis on adjacent channels. For example, to enable mirroring, corresponding slots on channel A and channel B must have DIMMS of identical parameters. But DIMMs on adjacent slots on the same channel do not need identical parameters.

If one socket fails the population requirements for RAS, the BIOS sets all six channels to the Channel Independent mode. One exception to this rule is when all DIMM slots from a socket are empty. E.g., when only sockets A1, B1, C1 are populated, mirroring is possible on the platform.

The memory slots of DDR3 channels from the Intel® Xeon® Processor 5500 Series and Intel® Xeon® Processor 5600 Series should be populated on a farthest first fashion. This holds true even in the Channel Independent mode. This means that A2 cannot be populated or used if A1 is empty.

3.2.4.2 Channel Independent Mode

In the Channel Independent mode, multiple channels can be populated in any order (e.g., channels B and C can be populated while channel A is empty). Also, DIMMs on adjacent channels need not have identical parameters. Therefore, all DIMMs are enabled and utilized in the Channel Independent mode.

Adjacent slots on a DDR3 channel from The Intel® Xeon® Processor 5500 Series and Intel® Xeon® Processor 5600 Series do not need matching size and organization. However the speed of the channel is configured to the maximum common speed of the DIMMs.

The single channel mode is established using the Channel Independent mode by populating DIMM slots from channel A only.

3.2.4.3 Channel Mirroring Mode

The Intel® Xeon® Processor 5500 Series and Intel® Xeon® Processor 5600 Series support channel mirroring to configure available channels of DDR3 DIMMS in the mirrored configuration. Unlike channel sparing, the mirrored configuration is a redundant image of the memory, and can continue to operate despite the presence of sporadic uncorrectable errors.

Channel mirroring is a RAS feature in which two identical images of memory data are maintained, thus providing maximum redundancy. On the Intel® Xeon® Processor 5500 Series and Intel® Xeon® Processor 5600 Series-based Intel® server boards, 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 and Intel® Xeon® Processor 5600 Series alternates between both channels for read transactions. Write transactions are issued to both channels under normal circumstances.

When the system is in the Channel Mirroring mode, channel C and channel F of socket 1 and socket 2 respectively are not used. Hence, the DIMMs populated on these channels are disabled and hence do not contribute to the available physical memory. For example, if the system is operating in Channel Mirroring mode and the total size of the DDR3 DIMMs is 1.5 GB (3 x 512 MB DIMMs), then the active memory is only 1 GB.

Because the available system memory is divided into a primary image and a copy of the image, the effective system memory is reduced by at least one-half. For example, if the system is operating in the Channel Mirroring mode and the total size of the DDR3 DIMMs is 1 GB, then the effective size of the memory is 512 MB because half of the DDR3 DIMMs are the secondary images.

For channel mirroring to work, participant DDR3 DIMMs on the same DIMM slots on the adjacent channels must be identical in terms of technology, number of ranks, and size. DIMMs within the channel do not need matching parameters.

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

3.2.4.3.1 Minimum DDR3 DIMM Population for Channel Mirroring

Memory mirroring has the following minimum requirements:

- **Channel configuration**: Mirroring requires the first two adjacent channels to be active.
- **Socket configuration**: Mirroring requires that both socket 1 and socket 2 DIMM population meets the requirements for mirroring mode. The platform BIOS configures the system in mirroring mode only if both nodes qualify. The only exception to this rule is socket 2 with all empty DIMM slots.

As a direct consequence of these requirements, the minimal DIMM population is {A1, B1}. In this configuration, processor cores on socket 2 suffer memory latency due to usage of remote memory from socket 1. An optimal DIMM population for channel mirroring in a DP server platform is {A1, B1, D1, and E1}. {A1, B1} must be identical and {D1, E1} must be identical. However, DIMMs do not need to be identical across sockets.

In this configuration, DIMMs {A1, B1} and {D1, E1} operate as (primary copy, secondary copy) pairs independent from each other. Therefore, the optimal number of DDR3 DIMMs for channel mirroring is a multiple of four, arranged as mentioned above. The BIOS disables all non-identical DDR3 DIMMs or pairs of DDR3 DIMMs across the channels to achieve symmetry and balance between the channels.

3.2.4.3.2 Mirroring DIMM Population Rules Variance across Nodes

Memory mirroring in The Intel® Xeon® Processor 5500 Series and Intel® Xeon® Processor 5600 Series-based platforms is channel mirroring. Mirroring is not done across sockets, so each socket may have a different memory configuration. Channel mirroring in socket 1 and socket 2 are mutually independent. As a result, if channel A and channel B have identical DIMM population, and channel D and channel E have identical DIMM population, then mirroring is possible even if the DIMM population is not identical for channel A and channel D.

For example, if the system is populated with six DIMMS {A1, B1, A2, B2, D1, E1}, channel mirroring is possible. Both the populations shown in the following table are valid.

Table 8. Mirroring DIMM Population Rules Variance across Nodes

A1	A2	B1	B2	C1	C2	D1	D2	E1	E2	F1	F2	Mirroring Possible?
P		P				P		P				Yes
P	P	P	P			P		P				Yes

3.2.5 Memory Upgrade Rules

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 and Intel® Xeon® Processor 5600 Series to maximize memory bandwidth

In the Channel Independent mode, all DDR3 channels operate independently. The Channel Independent mode can also be used to support a single DIMM configuration in channel A and in the single channel mode.

The following general rules must be observed when selecting and configuring memory to obtain the best performance from the system.

- Mixing RDIMMs and UDIMMs is not supported.
- 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.
- When CPU Socket 1 is empty, any DIMM memory in Channel A through Channel C is unavailable.
- When CPU Socket 2 is empty, any DIMM memory in Channel D through Channel F is unavailable.
- If both processor sockets are populated but Channel A through Channel C is empty, the platform can still function with remote memory in Channel D through Channel F. However, platform performance suffers latency due to remote memory.
- The memory operational mode is configurable at the channel level. Two modes are supported: Independent Channel and Mirrored Channel.
- The memory slots of each DDR3 channel from the Intel® Xeon® Processor 5500 Series and Intel® Xeon® Processor 5600 Series are populated on a farthest first fashion. This holds true even for the Independent Channel mode. Therefore, if A1 is empty, A2 cannot be populated or used.
- The BIOS selects Independent Channel mode by default, which enables all installed memory on all channels simultaneously.
- Mirrored Channel mode is not available when only one processor is populated (CPU Socket 1).
- If both processor sockets are populated and the installed DIMMs are associated with both processor sockets, then a given RAS mode is selected only if both the processor sockets are populated to conform to that mode.
- The minimum memory population possible is one DIMM in slot A1. In this configuration, the system operates in the Independent Channel mode. RAS is not available.

- If both processor sockets are populated, the next upgrade from the Single Channel mode installs DIMM_D1. This configuration results in an optimal memory thermal spread, as well as Non-Uniform Memory Architecture (NUMA) aware interleaving. The BIOS selects the Independent Channel mode of operation.
- If only one processor socket is populated, the next upgrade from the Single Channel mode is installing DIMM_B1 to allow channel interleaving. The system operates in the Independent Channel mode.
- The DIMM parameter-matching requirements for memory RAS is local to a socket. For example, while Channels A/B/C can have one match of timing, technology, and size, Channels D/E/F can have a different set of parameters and RAS still functions.
- DDR3 DIMMs on adjacent slots on the same channel do not need to be identical.
- For the Mirrored Channel mode, the memory in Channels A and B of Socket 1 must be identical and Channel C should be empty. Similarly, the memory in Channels D and E of Socket 2 must be identical and Channel F should be empty.
  a. The minimum population upgrade for the Mirrored Channel mode is DIMM_A1, DIMM_B1, DIMM_D1, and DIMM_E1 with both processor sockets populated. DIMM_A1 and DIMM_B1 as a pair must be identical, and so must DIMM_D1 and DIMM_E1, but the DIMMs on different processor sockets do not need to be identical. Failing to comply with these rules results in a switch back to the Independent Channel mode.
  b. If Mirrored Channel mode is selected and the third channel of each processor socket is not empty, the BIOS disables the memory in the third channel of each processor socket.
- In the Mirrored Channel mode, both sockets must simultaneously satisfy the DIMM matching rules on their respective adjacent channels. If the DDR3 DIMMs on adjacent channels of a socket are not identical, the BIOS configures both the processor sockets to default to the Independent Channel mode. If DIMM_D1 and DIMM_E1 are not identical, then the system switches to the Independent Channel Mode

3.3 Intel® 5520 Chipset IOH

The Intel® 5520 Chipset component is an I/O Hub (IOH.) The Intel® 5520 Chipset provides a connection point between various I/O components and Intel® processors via the Intel® QPI interface.

The Intel® 5520 Chipset IOH is capable of interfacing with up to 36 PCI Express* lanes, which can be configured in various combinations of x4, x8, x16 and limited x2 and x1 devices.

The Intel® 5520 Chipset IOH is responsible for providing a path to the legacy bridge. In addition, Intel® 5520 Chipset supports a x4 DMI (Direct Media Interface) link interface for the legacy bridge, and interfaces with other devices through SMBus, Controller Link and RMII manageability interfaces. The Intel® 5520 Chipset supports the following features and technologies:

- Intel® QuickPath Interconnect (Intel® QPI)
- PCI Express* Gen2
- Intel® I/O Acceleration Technology 2 (Intel® I/OAT2)
- Intel® Virtualization Technology (Intel® VT) for Directed I/O 2 (Intel® VT-d2)

3.4 Intel® 82801Jx I/O Controller Hub (ICH10R)

The Intel® 82801Jx I/O Controller Hub (ICH10R) provides extensive I/O support and provides the following functions and capabilities:

- *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; 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 PCI Subsystem

The primary I/O buses for the Intel® Server Board S5520UR, S5520URT are PCI, PCI Express* Gen1 and PCI Express* Gen2 with six 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 Gbit/s one direction per lane for Gen1 and 5.0 Gbit/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, etc.). 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 table lists the characteristics of the PCI bus segments. Details about each bus segment follow the tables.

Table 9. Intel® Server Board S5520UR, S5520URT PCI Bus Segment Characteristics

PCI Bus Segment	Voltage	Width	Speed	Type	PCI I/O Card Slots
Port 0 ICH10R	3.3 V	x4	10 Gb/s	PCI Express* Gen1	x4 PCI Express* Gen1 throughput to the Intel® 5520 Chipset IOH
Port 5 ICH10R	3.3 V	x1	2.5 Gb/s	PCI Express* Gen1	x4 PCI Express* Gen1 throughput to an on-board Integrated BMC
Port 1-4 ICH10R	3.3 V	x4	10 Gb/s	PCI Express* Gen1	x4 PCI Express* Gen1 throughput to a midplane in the Intel® Server Chassis. Uses bridge board for connection.
PE1, PE2 Intel® 5520 Chipset IOH PCI Express*	3.3 V	x4	10 Gb/s	PCI Express* Gen1	x4 PCI Express* Gen1 throughput to an on-board NIC.
PE3, PE4 Intel® 5520 Chipset IOH PCI Express*	3.3 V	x8	40 Gb/S	PCI Express* Gen2	x8 PCI Express* Gen2 throughput to the riser slot.
PE5, PE6 Intel® 5520 Chipset IOH PCI Express*	3.3 V	x8	40 Gb/S	PCI Express* Gen2	x8 PCI Express* Gen2 throughput to the riser slot.
PE7, PE8 Intel® 5520 Chipset IOH PCI Express*	3.3 V	x8	40 Gb/S	PCI Express* Gen2	x8 PCI Express* Gen2 throughput to the riser slot.
PE9, PE10 Intel® 5520 Chipset IOH PCI Express*	3.3 V	x8	40 Gb/S	PCI Express* Gen2	x4 PCI Express* Gen2 throughput to each of the two IO Module Mezzanine connectors.

3.4.2 Serial ATA Support

The ICH10R has an integrated Serial ATA (SATA) controller that supports independent DMA operation on six ports and data transfer rates of up to 3.0 Gb/s. The six SATA ports on the server board are numbered SATA-0 through SATA-5. The SATA ports can be enabled or disabled and/or configured by accessing the BIOS setup utility during POST.

3.4.2.1 Software RAID Support

The on-board storage capability of these server boards includes support for Intel® Embedded Server RAID Technology II (Intel® ESRTII), which provides three standard software RAID levels: Data stripping (RAID Level 0), data mirroring (RAID Level 1), and data stripping with mirroring (RAID Level 10). For higher performance, you can use data stripping to alleviate disk bottlenecks by taking advantage of the dual independent DMA engines that each SATA port offers. Data mirroring is used for data security. Should a disk fail, a mirrored copy of the failed disk is brought online. There is no loss of either PCI resources (request/grant pair) or add-in card slots.

With the addition of an optional Intel® RAID Activation Key, Intel® ESRTII is also capable of providing fault tolerant data stripping (software RAID Level 5), such that if a SATA hard drive fails, you can restore the lost data on a replacement drive from the other drives that make up the RAID 5 pack.

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

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

3.4.2.2 Software RAID 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 as well as to detect any faults in the Intel® Embedded Server RAID Technology II volume(s).

3.4.3 USB 2.0 Support

The USB controller functionality integrated into ICH10R provides the server board 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 board.
- One internal 2x5 header (J1J2) is provided, capable of supporting two optional USB 2.0 ports.
- Two ports are routed over the bridge board for chassis front panel USB ports and/or a USB floppy drive. Due to the long route distance, those two ports are only capable of supporting low-speed and full-speed modes.

- One internal low-profile 2x5 header (J1J1) is provided to support low-profile USB solid state drives.

3.5 I/O Module

The Intel® Server Board S5520UR, S5520URT supports a variety of I/O Module options using 2 x4 PCI Express* Gen2 Mezzanine connectors on the rear of the server board. For more information on these modules, see the *Intel® Server Board S5520UR*, S5520URT *I/O Module Hardware Specification*.

Note: The Intel® I/O Module AXX4SASMOD does not support the Intel® Embedded Server RAID Technology II implementation and only the Intel® IT/IR RAID is supported and would be the only available setting under BIOS.

3.6 Integrated Baseboard Management Controller

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

The following is a summary of the Integrated BMC management hardware features utilized by the ServerEngines* LLC Pilot II Integrated BMC:

- IPMI 2.0 Compliant
- Integrated 250 Mhz 32-bit ARM9 processor
- Six I^2C SMBus modules with Master-Slave support
- Two independent 10/100 Ethernet Controllers with RMII support
- Six I^2C interface
- Memory Management Unit (MMU)
- DDR2 16-bit up to 667 MHz memory interface
- Dedicated real-time clock for Integrated BMC
- Up to 16 direct and 64 Serial GPIO ports
- 12 10-bit Analog to Digital Converters
- Eight Fan Tachometers Inputs
- Four Pulse Width Modulators (PWM)
- Chassis Intrusion Logic with battery backed general purpose register
- JTAG Master interface
- Watchdog timer

Additionally, the ServerEngines* Pilot II part integrates a super I/O module with the following features:

- Keyboard Style/BT Interface
- Two 16C550 compatible serial ports
- Serial IRQ support

- 16 GPIO ports (shared with Integrated BMC)
- LPC to SPI Bridge for system BIOS support
- SMI and PME support
- ACPI compliant
- Wake-up control

The Pilot II contains an integrated KVMS subsystem and graphics controller with the following features:

- USB 2.0 for keyboard, mouse, and storage devices
- Hardware Video Compression for text and graphics
- Hardware encryption
- 2D Graphics Acceleration
- DDR2 graphics memory interface
- Up to 1600x1200 pixel resolution

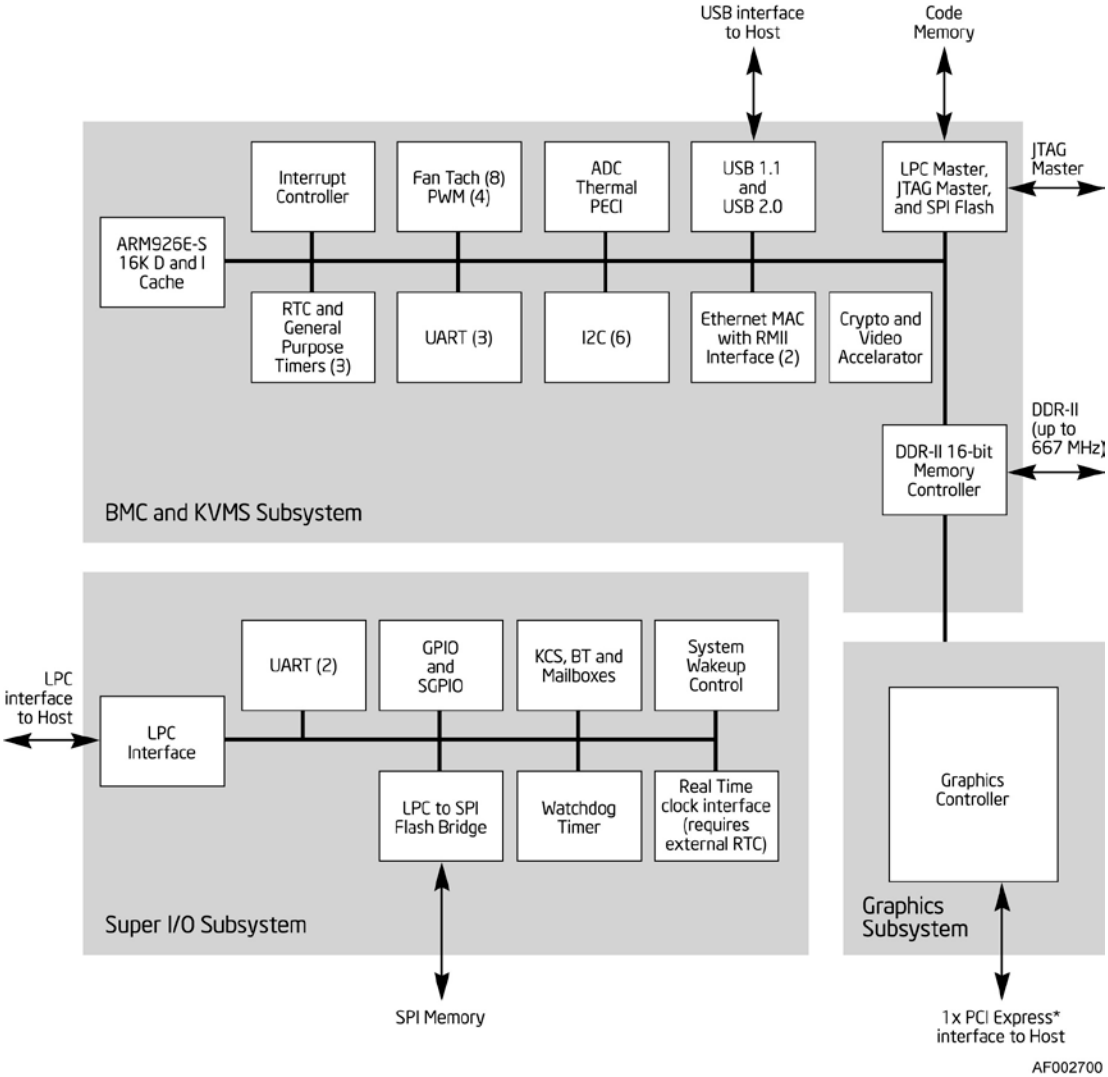


Figure 12. Integrated BMC Hardware

3.6.1 Integrated BMC Embedded LAN Channel

The Integrated BMC hardware includes two dedicated 10/100 network interfaces. These interfaces are not shared with the host system. At any time, only one dedicated interface may be enabled for management traffic. The default active interface is the NIC 1 port.

For these channels, support can be enabled for IPMI-over-LAN and DHCP.

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

- IP Address: Static.
- All users disabled.

3.6.2 Floppy Disk Controller

The server board does not support a floppy disk controller interface. However, the system BIOS recognizes USB floppy devices.

3.6.3 Keyboard and Mouse Support

The server board does not support PS/2 interface keyboards and mice. However, the system BIOS recognizes USB specification-compliant keyboard and mice.

3.6.4 Wake-up Control

The super I/O contains functionality that allows various events to power on and power off the system.

3.7 Video Support

The server board includes a video controller in an on-board Server Engines* Integrated Baseboard Management Controller along with 8 MB of video DDR2 SDRAM. The SVGA subsystem supports a variety of modes, up to 1600 x 1200 resolution in 8/16 bpp modes under 2D. It also supports both CRT and LCD monitors up to 85 Hz vertical refresh rate.

The video is accessed using a standard 15-pin VGA connector (J8A1) found on the back edge of the server board. The on-board video controller can be disabled using the BIOS Setup utility or when an add-in video card is detected. The system BIOS provides the option for dual-video operation when an add-in video card is configured in the system.

3.7.1 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 10. Video Modes

2D Mode Resolution	2D Video Mode Support (Color Bit)				
	8 bpp	16 bpp	24 bpp	32 bpp	
640x480	Supported	Supported	Supported	Supported	
	60, 72, 75, 85	60, 72, 75, 85	60, 72, 75, 85	60, 72, 75, 85	Monitor Refresh Rate (Hz)
800x600	Supported	Supported	Supported	Supported	
	56, 60, 72, 75, 85	56, 60, 72, 75, 85	56, 60, 72, 75, 85	56, 60, 72, 75, 85	Monitor Refresh Rate (Hz)
1024x768	Supported	Supported	Supported	Supported	
	60, 70, 75, 85	60, 70, 75, 85	60, 70, 75, 85	60, 70, 75, 85	Monitor Refresh Rate (Hz)
1152x864	Supported	Supported	Supported	N/A	
	75	75	75	N/A	Monitor Refresh Rate (Hz)
1280x1024	Supported	Supported	Supported	N/A	
	60, 75, 85	60, 75, 85	60	N/A	Monitor Refresh Rate (Hz)
1440x900	Supported	Supported	Supported	N/A	
	60	60	60	N/A	Monitor Refresh Rate (Hz)
1600x1200	Supported	Supported	N/A	N/A	
	60, 65, 70, 75, 85	60, 65, 70	N/A	N/A	Monitor Refresh Rate (Hz)

3.7.2 Dual Video

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

- In the single mode (dual monitor video = disabled), the on-board video controller is disabled when an add-in video card is detected.
- In the dual mode (on-board video = enabled, dual monitor video = enabled), the on-board video controller is enabled and is the primary video device. The external video card is allocated resources and is considered the secondary video device. The BIOS Setup utility provides options to configure the feature as follows:

Table 11. Video mode

On-board Video	**Enabled** Disabled	

Dual Monitor Video	**Enabled** Disabled	Shaded if on-board video is set to "Disabled"

3.8 Network Interface Controller (NIC)

Network interface support is provided from the on-board Intel® 82575EB NIC, which is a single, compact component with two fully integrated GbE Media Access Control (MAC) and Physical Layer (PHY) ports. The on-board Intel® 82575EB NIC provides the server board with support for dual LAN ports designed for 10/100/1000 Mbps operation.

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

Each network interface controller (NIC) drives two LEDs located on each network interface connector (J6A1, J5A2). The link/activity LED (at the right of the connector) indicates network connection when on, and transmit/receive activity when blinking. The speed LED (at the left 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 12. NIC2 Status LED

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

3.8.1 MAC Address Definition

Each Intel® Server Board S5520UR, S5520URT has the following four MAC addresses assigned to it at the Intel® factory.

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

During the manufacturing process, each server board has a white MAC address sticker included with the board. The sticker displays the NIC 1 MAC address in both bar code and alphanumeric formats, and displays the Intel® RMM3 MAC address in alphanumeric format.

3.9 Trusted Platform Module (TPM) – Supported only on S5520URT

3.9.1 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 S5520URT 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).

3.9.2 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.

3.9.2.1 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).

3.9.2.2 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.

3.9.2.3 Security Screen

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

> Press <F2> to enter setup

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

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

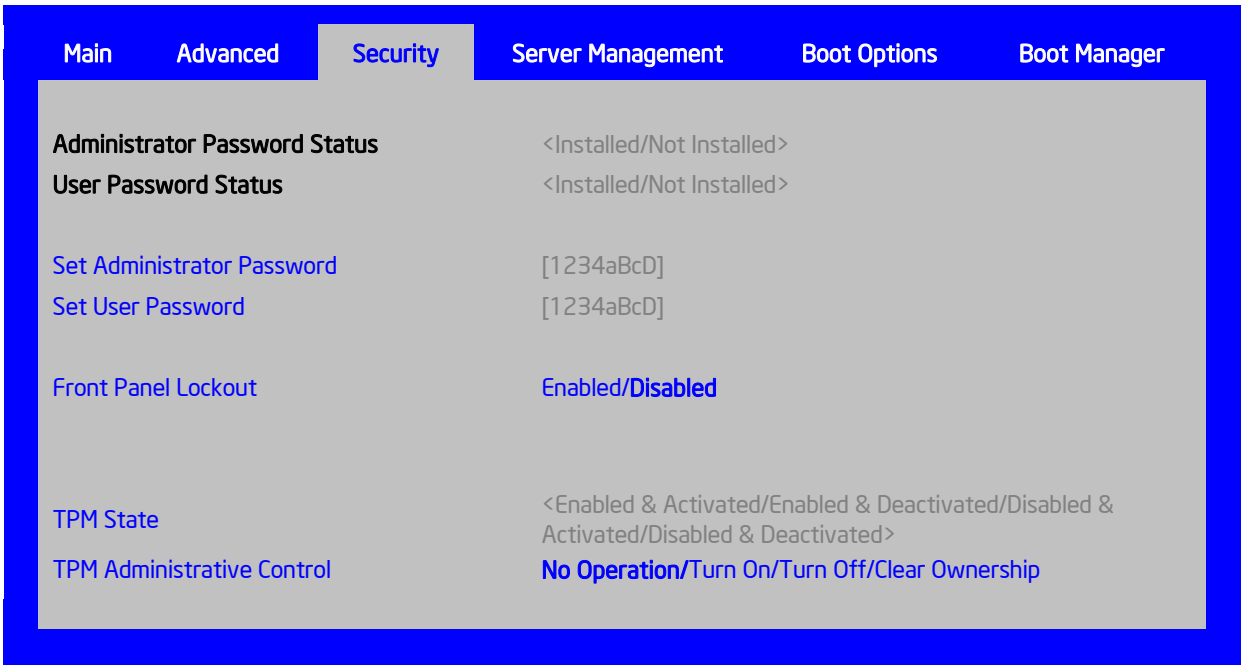


Figure 13. Setup Utility – TPM Configuration Screen

Table 13. TSetup Utility – Security Configuration Screen Fields

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

3.9.3 Intel® Trusted Execution Technology (Intel® TXT)

3.9.3.1 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.

3.9.3.2 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. 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. 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.

3.9.3.3 Enabling Intel® TXT on Intel® Server Board

Intel® TXT can be supported by Intel® Server Board S5520URT (PBA# E81084-752 or later version), following steps describe how to set up Intel® TXT feature:

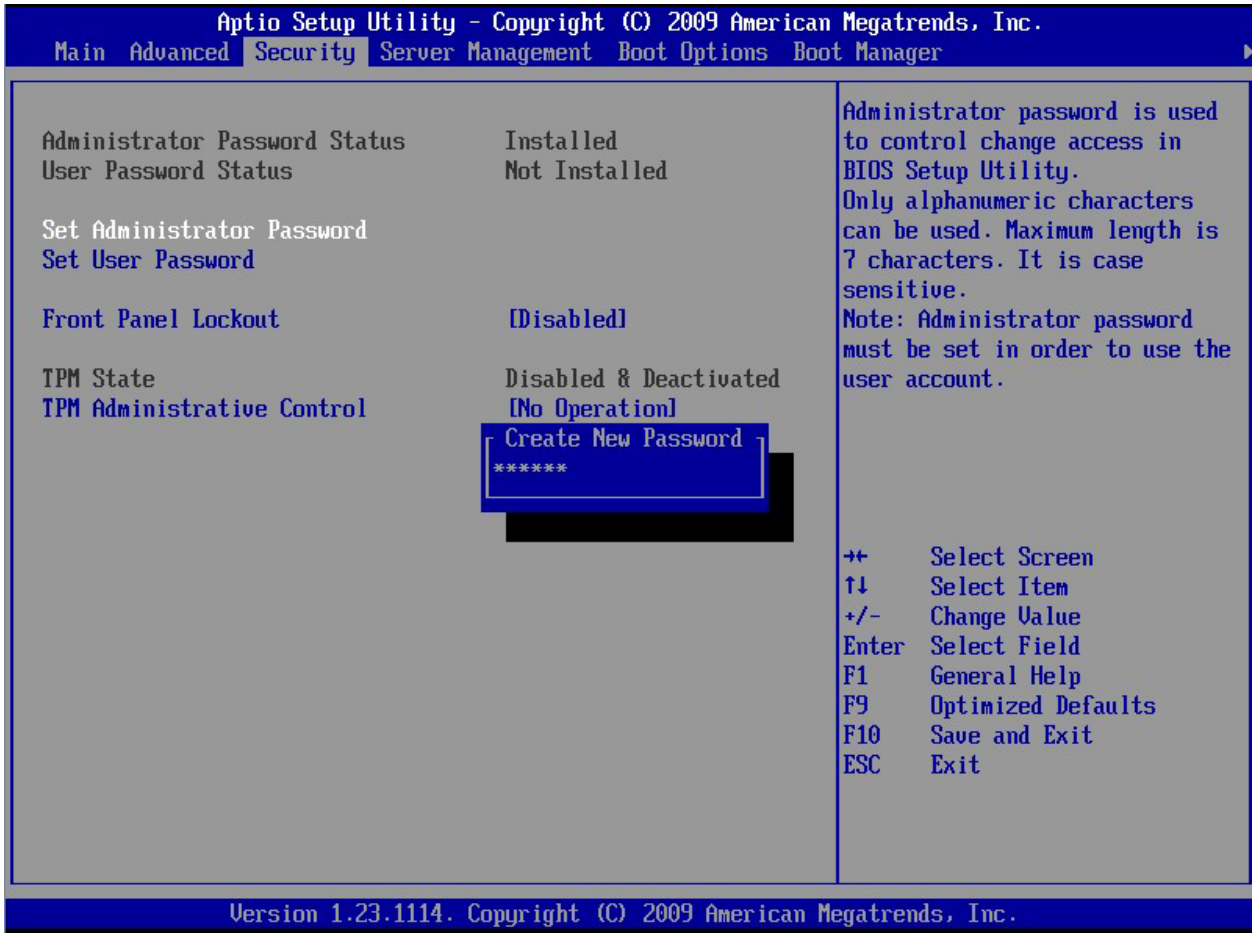
System pre-requirements:

- Processor: B1 or later stepping Intel® Xeon Processor 5600 Series
- Server Board: Intel® Server Board S5520URT; PBA version E81084-752 or later
- Memory: At least 1 GB memory installed

Intel® TXT Setup:

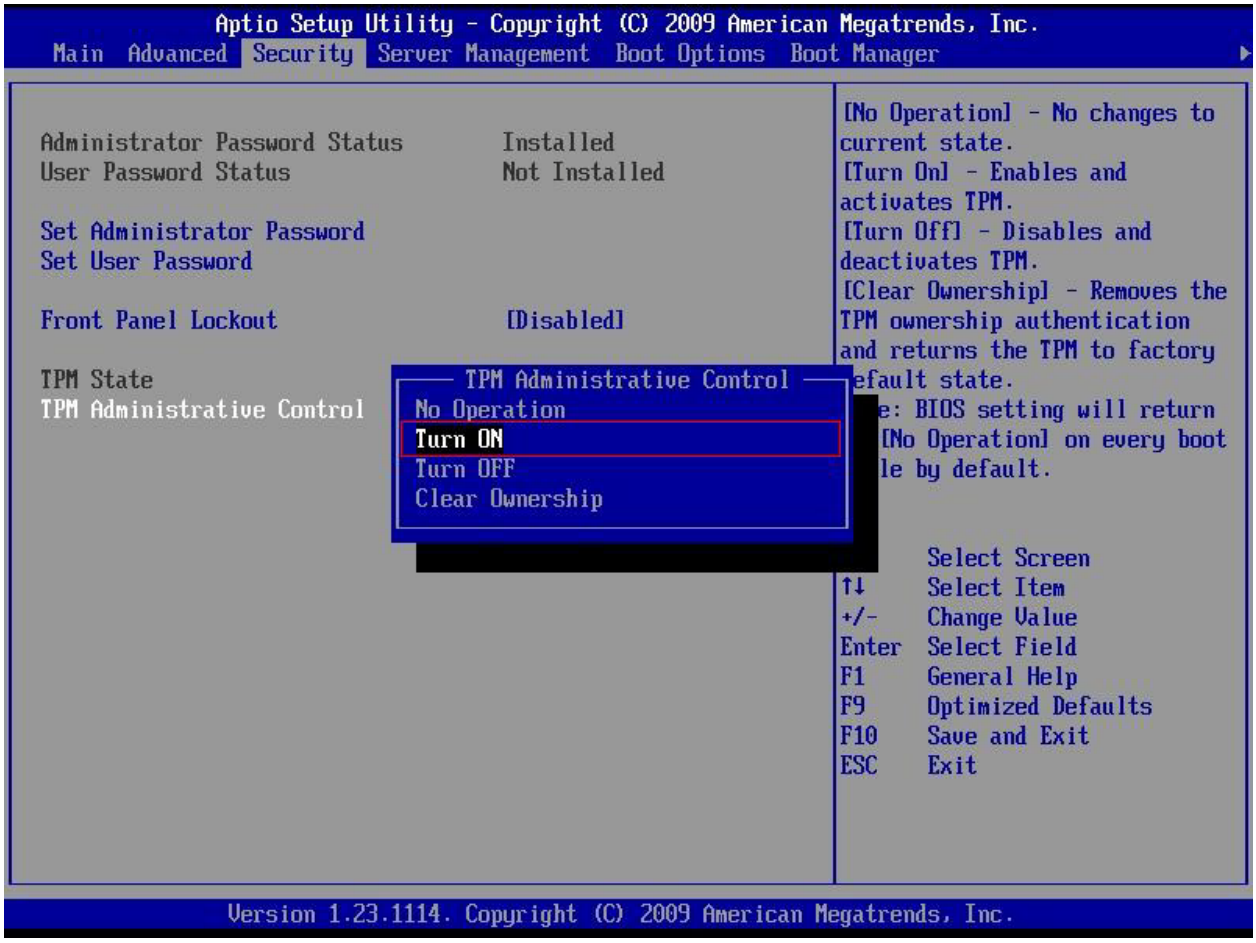
Enable TPM module:

1. Go to BIOS setup Menu page, Security Tab, set administrator password



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.



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

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

The Intel® Virtualization Technology is designed to support multiple software environments sharing same hardware resources. Each software environment may consist of an OS and applications. The Intel® Virtualization Technology can be enabled or disabled in the BIOS setup. The default behavior is disabled.

Note: If the setup options are changed to enable or disable the Virtualization Technology setting in the processor, the user must perform an AC power cycle for the changes to take effect.

The Intel® 5520 Chipset IOH supports 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.

4. Platform Management

The platform management subsystem is based on the Integrated BMC features of the ServerEngines* Pilot II. The on-board platform management subsystem consists of communication buses, sensors, system BIOS, and server management firmware. The following diagram provides an overview of the Server Management Bus (SMBus) architecture used on this server board.

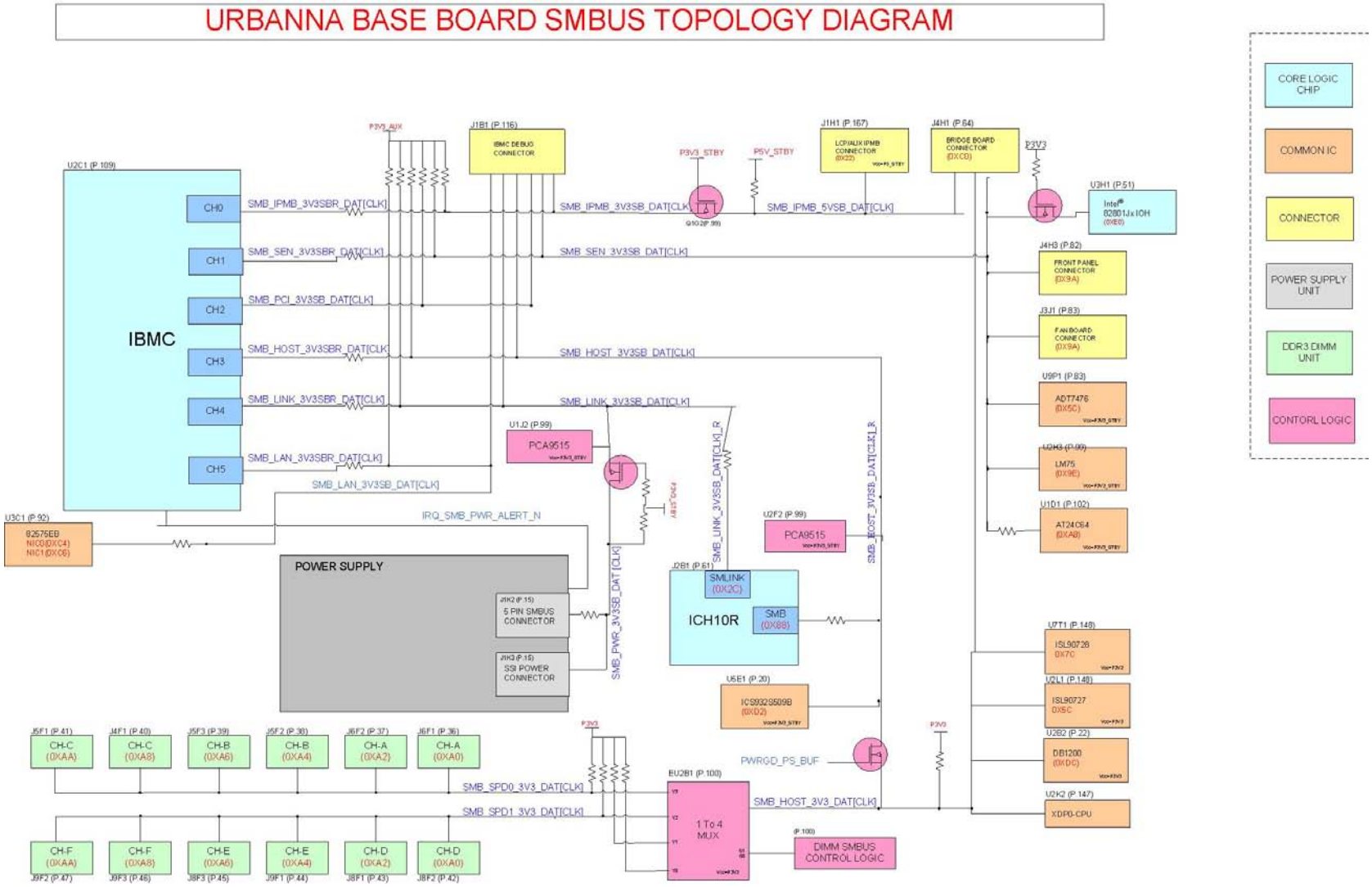


Figure 14. Server Management Bus (SMBus) Block Diagram

4.1 Feature Support

4.1.1 IPMI 2.0 Features

- Integrated Baseboard Management Controller (Integrated 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 Integrated BMC receives and processes events from other platform subsystems.
- Field replaceable unit (FRU) inventory device functionality: The Integrated BMC supports access to system FRU devices using IPMI FRU commands.
- System event log (SEL) device functionality: The Integrated BMC supports and provides access to a SEL.
- Sensor device record (SDR) repository device functionality: The Integrated BMC supports storage and access of system SDRs.
- Sensor device and sensor scanning/monitoring: The Integrated 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).
- Terminal mode serial interface.
- IPMB interface.
- LAN interface that supports the IPMI-over-LAN protocol (RMCP, RMCP+).
- Serial-over-LAN (SOL).
- ACPI state synchronization: The Integrated BMC tracks ACPI state changes that are provided by the BIOS.
- Integrated Baseboard Management Controller (Integrated BMC) self test: The Integrated BMC performs initialization and run-time self tests, and makes results available to external entities.

See also the *IPMI 2.0 Specification*.

4.1.2 Non-IPMI Features

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

- In-circuit Integrated BMC firmware update.
- Fault resilient booting (FRB): FRB2 is supported by the watchdog timer functionality
- Chassis intrusion detection and chassis intrusion cable presence detection.
- 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: Support for multiple fan profiles.
- Signal testing support: The Integrated Baseboard Management Controller (Integrated BMC) provides test commands for setting and getting platform signal states.
- The Integrated Baseboard Management Controller (Integrated BMC) generates diagnostic beep codes for fault conditions.
- System GUID storage and retrieval.
- Front panel management: The Integrated Baseboard Management Controller (Integrated 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 Integrated Baseboard Management Controller (Integrated 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 Integrated BMC sends and responds to ARPs (supported on embedded NICs)
- Dynamic Host Configuration Protocol (DHCP): The Integrated BMC performs DHCP (supported on embedded NICs).
- Chassis intrusion fan interactions.
- Platform environment control interface (PECI) thermal management support.

4.2 Optional Advanced Management Feature Support

This section explains the advanced management features supported by the Integrated Baseboard Management Controller (Integrated BMC) firmware.

4.2.1 Enabling Advanced Management Features

The Integrated BMC enables the 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® RMM3

The Intel® RMM3 provides the Integrated 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 like Web Services for Management (WS-MAN).

4.2.2 Keyboard, Video, Mouse (KVM) Redirection

The Integrated BMC firmware supports keyboard, video, and mouse redirection over LAN. This feature is available remotely from the embedded web server as a Java applet. This feature is enabled only when the Intel® RMM3 is present.

4.2.2.1 Keyboard and Mouse

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

4.2.2.2 Video

Video output from the KVM subsystem is equivalent to the video output on the local console. Video redirection is available after video is initialized by the system BIOS.

4.2.2.3 Availability

Up to two remote KVM sessions are supported. The default inactivity timeout is 30 minutes, but may be changed through the embedded web server. Remote KVM activation does not disable the local system keyboard, video, or mouse. Remote KVM is not deactivated by local system input, unless the feature is disabled locally.

KVM sessions 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. This may be used in conjunction with the remote KVM feature, or as a standalone applet. This feature is enabled only when the Intel® RMM3 is present.

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 USB device to the server. Once mounted, the remote device appears just like a local device to the server, allowing system administrators or users to install software (including Operating systems, copy files, update BIOS, etc.) or boot the server from this device. USB 2.0 needs to be supported for better performance.

The following capabilities are supported:

- The operation of remotely mounted devices is independent of the local devices on the server. Both remote and local devices are useable in parallel.
- Either an IDE (CD-ROM, floppy) or USB device can be mounted as a remote device to the server.
- All supported (P1) Microsoft Windows* and Linux* operating systems can be booted from the remotely mounted device and from disk IMAGE (*.IMG) files.
- At least two devices can be mounted concurrently.
- The mounted device is visible to (and useable by) managed system's OS and BIOS in both pre-boot and post-boot states.
- The mounted device shows up in the BIOS boot order and the BIOS boot order can be changed to boot from this remote device.
- The operating system can be installed on a bare metal (no OS present) server using the remotely mounted device. This may also require the use of KVM redirection to configure the OS during install.

4.2.3.1 Availability

The default inactivity timeout is 30 minutes, but may be changed through the embedded web server.

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

4.2.4 Web Services for Management (WS-MAN)

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

4.2.5 Lightweight Directory Authentication Protocol (LDAP)

The Integrated BMC firmware supports the Local Directory Authentication Protocol (LDAP) protocol for user authentication.

Note: IPMI users/passwords and sessions are not supported over LDAP.

4.2.6 Embedded Webserver

The Integrated 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 – Limited control based on IPMI user privilege.
- Sensor Reading – Limited access based on IPMI user privilege.
- SEL Reading – Limited access based on IPMI user privilege.
- KVM/Media Redirection – Limited access based on IPMI user privilege. Only available when the Intel® RMM3 is present.
- IPMI User Management – Limited access based on IPMI user privilege.

The web server is available on all enabled LAN channels.

See Appendix B for Integrated BMC core sensors

4.3 Management Engine (ME)

4.3.1 Overview

Intel® Server Platform Services (SPS) is a set of manageability services provided by the firmware executing on an embedded ARC controller within the IOH. This management controller is also commonly referred to as the Management Engine (ME). The functionality provided by the Intel® SPS firmware is different from Intel® Active Management Technology (Intel® AMT) provided by the ME on client platforms.

Intel® Server Platform Services are value-add platform management options that enhance the value of Intel® platforms and their component ingredients (CPUs, chipsets and I/O components). Each service is designed to function independently wherever possible, or grouped together with one or more features in flexible combinations to allow OEMs to differentiate platforms.

4.3.2 Management Engine Firmware Update

The Management Engine (ME) Firmware (FW) provides a set of IPMI OEM commands for performing the FW update. An update utility running on the host uses IPMI bridging functionality to send these commands to the ME through the Integrated BMC over the Integrated BMC/IPMB link.

On Intel® server platforms, the ME FW uses a single operational image with a recovery image. In order to upgrade an operational image, the system must be booted from a recovery image. The recovery image only provides the basic functionality that is required to perform the update. Other SPS features are therefore not functional when the update is in progress.

4.3.3 Management Engine Interaction

Management Engine-Integrated BMC interactions include the following:

- Integrated BMC stores sensor data records for ME-owned sensors.
- Integrated BMC participates in ME firmware update.
- Integrated BMC initializes ME-owned sensors based on SDRs.
- Integrated BMC receives platform event messages sent by the ME.
- Integrated BMC notifies ME of POST completion.
- Integrated BMC may be queried by the ME for inlet temperature readings.

Integrated BMC utilizes the ICH10R fan tachs through the ME.

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 displays. 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 screens display.

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® workstation 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 14. 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 15. 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 affect if a sub-menu or pick list is displayed.
<Tab>	Select Field	The <Tab> key is used to move between fields. For example, <Tab> can be used 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.

Key	Option	Description
<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. The BIOS Setup screen does *not* display these values in bold. 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 needs to 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.

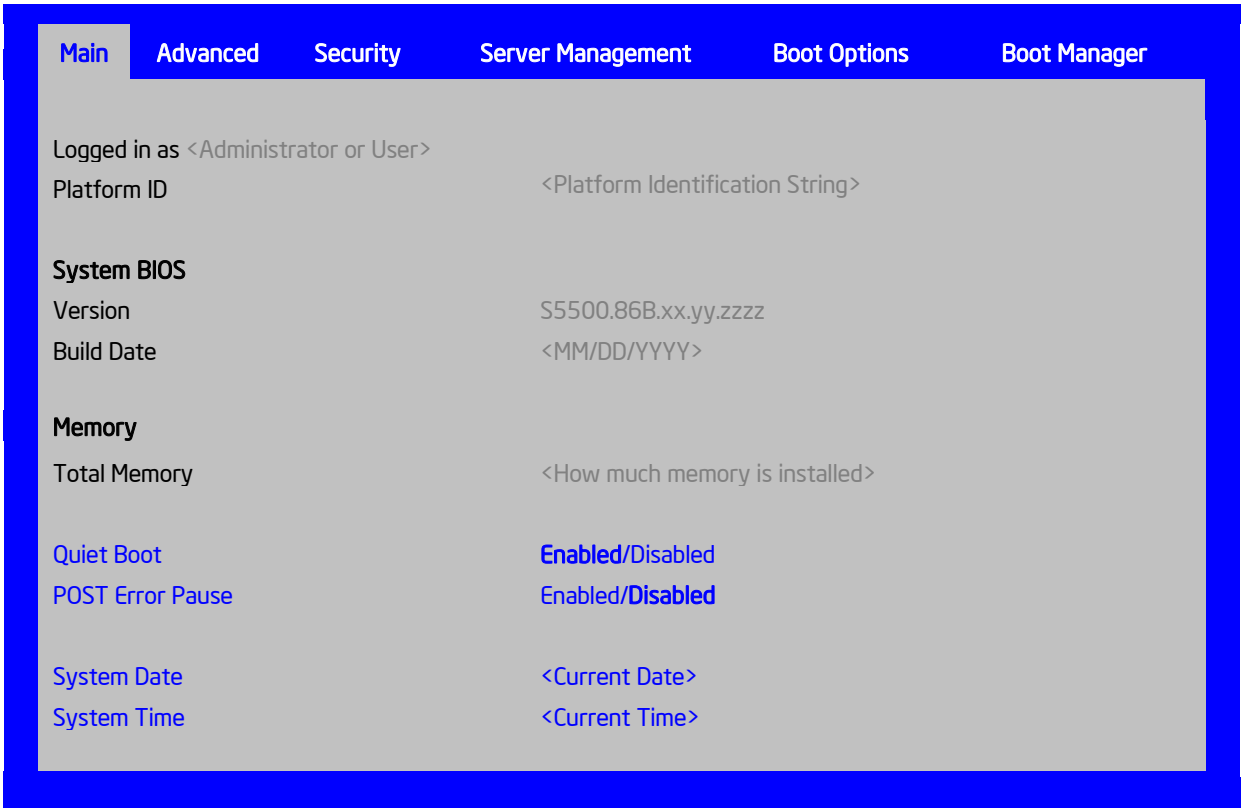


Figure 15. Setup Utility — Main Screen Display

Table 16. 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.

Setup Item	Options	Help Text	Comments
Memory			
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. This setting does not affect minor and fatal error displays.
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 want to 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.

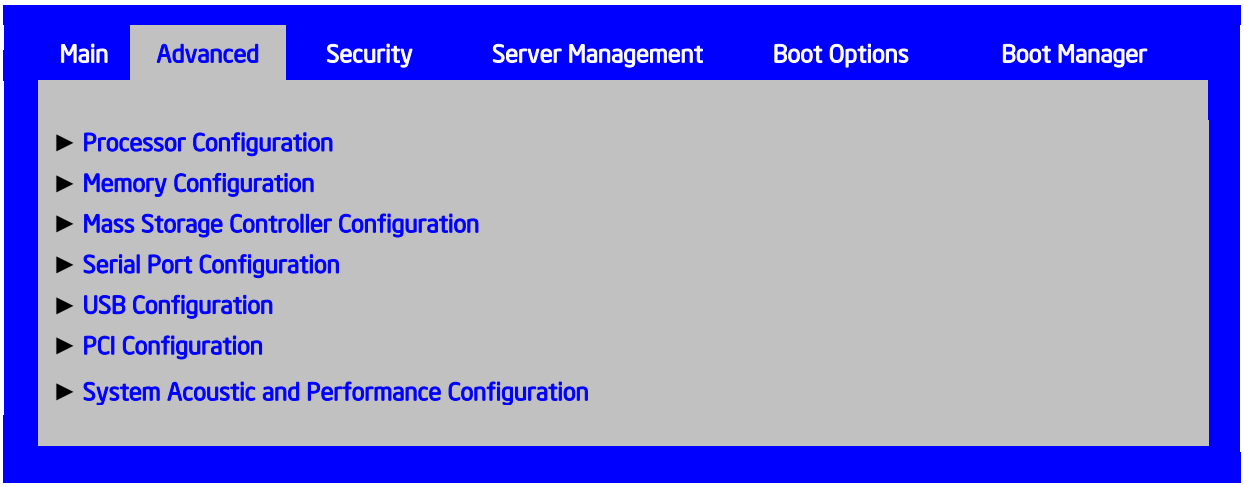


Figure 16. Setup Utility — Advanced Screen Display

Table 17. 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	
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 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 17. Setup Utility — Processor Configuration Screen Display

Table 18. 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 the QPI Link is using.
Intel® QPI Link Frequency			Information only. Current frequency the QPI Link is using.
Intel® Turbo Boost Technology	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.	

Setup Item	Options	Help Text	Comments
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.	
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**.

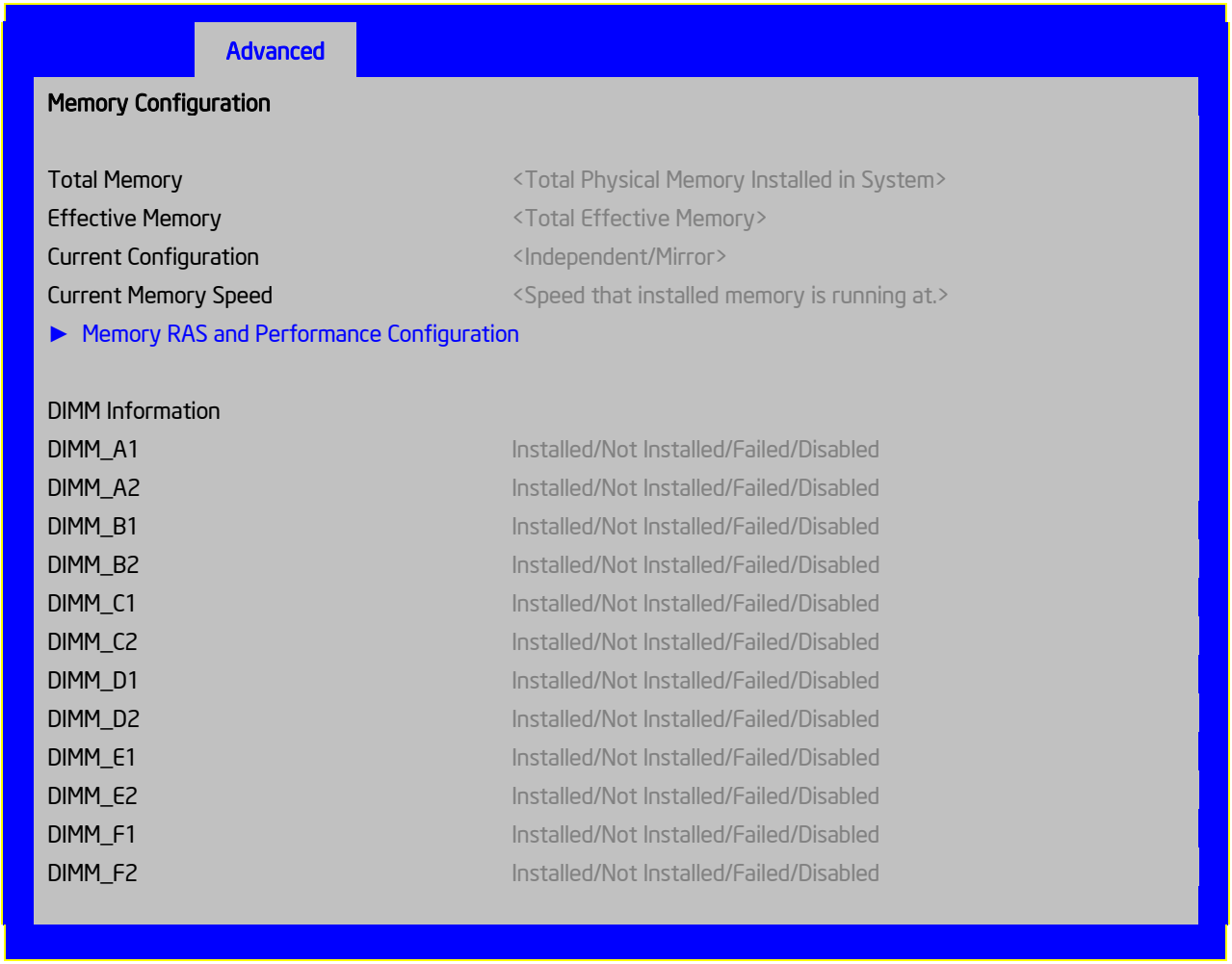


Figure 18. Setup Utility — Memory Configuration Screen Display

Table 19. 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**.

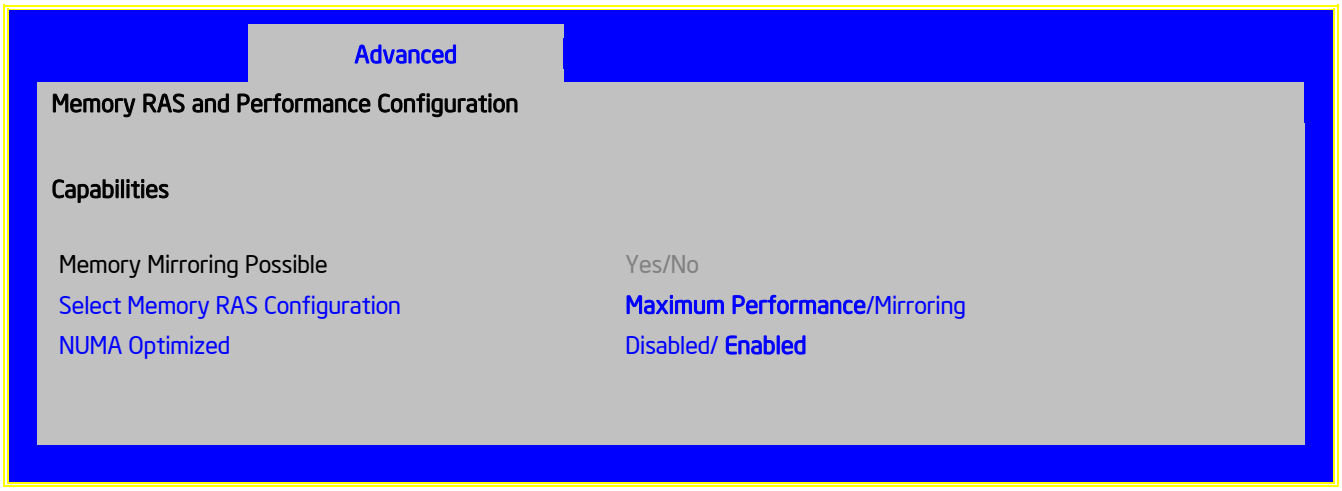


Figure 19. Setup Utility — Configure RAS and Performance Screen Display

Table 20. 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**.

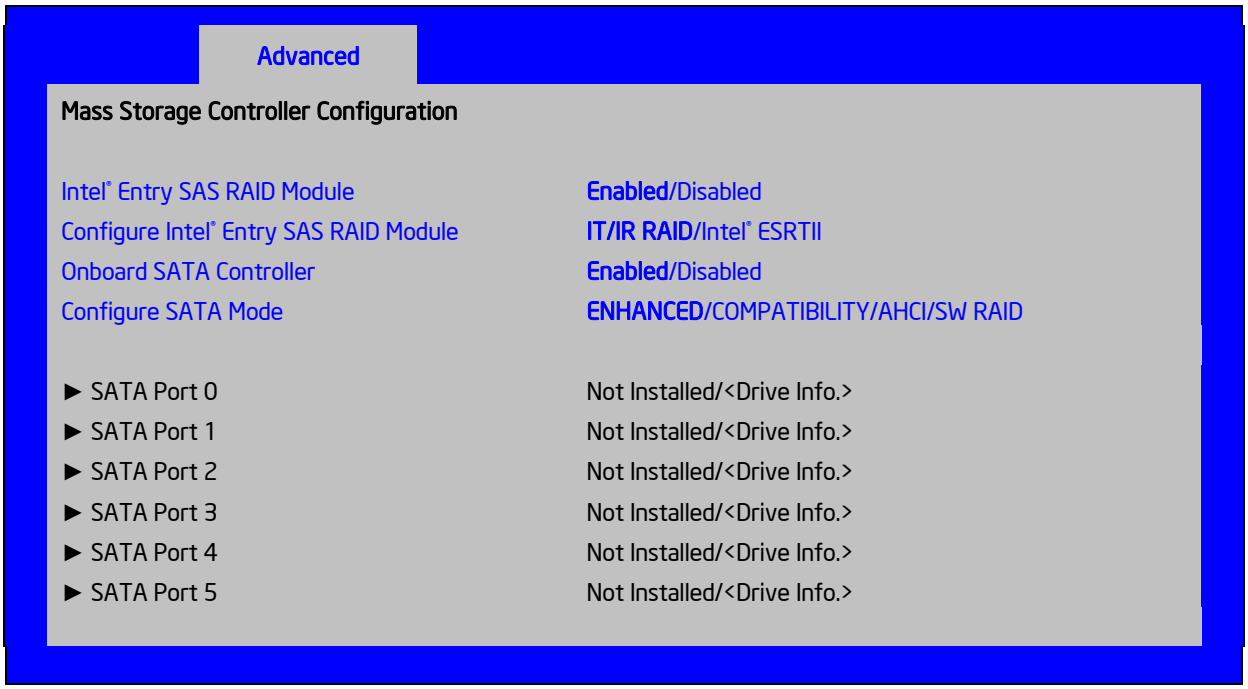


Figure 20. Setup Utility — Mass Storage Controller Configuration Screen Display

Table 21. 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.	Disappears when the Onboard SATA Controller is disabled. Changing this setting requires a reboot before you can set HDD boot order. [SW RAID] option is unavailable when EFI Optimized Boot is Enabled. You can only use SW RAID 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**.

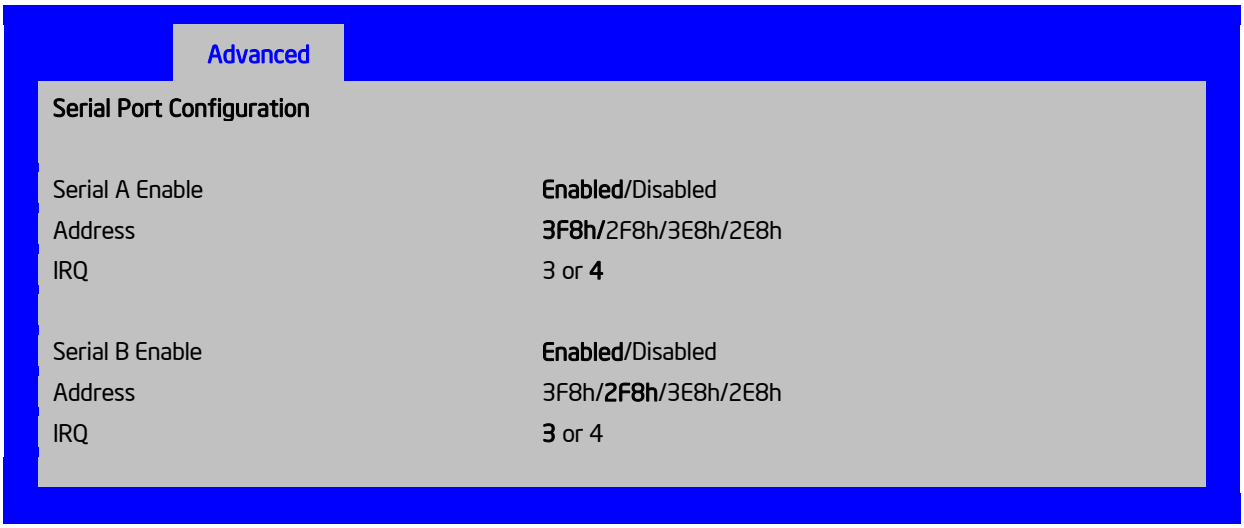


Figure 21. Setup Utility — Serial Port Configuration Screen Display

Table 22. 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**.

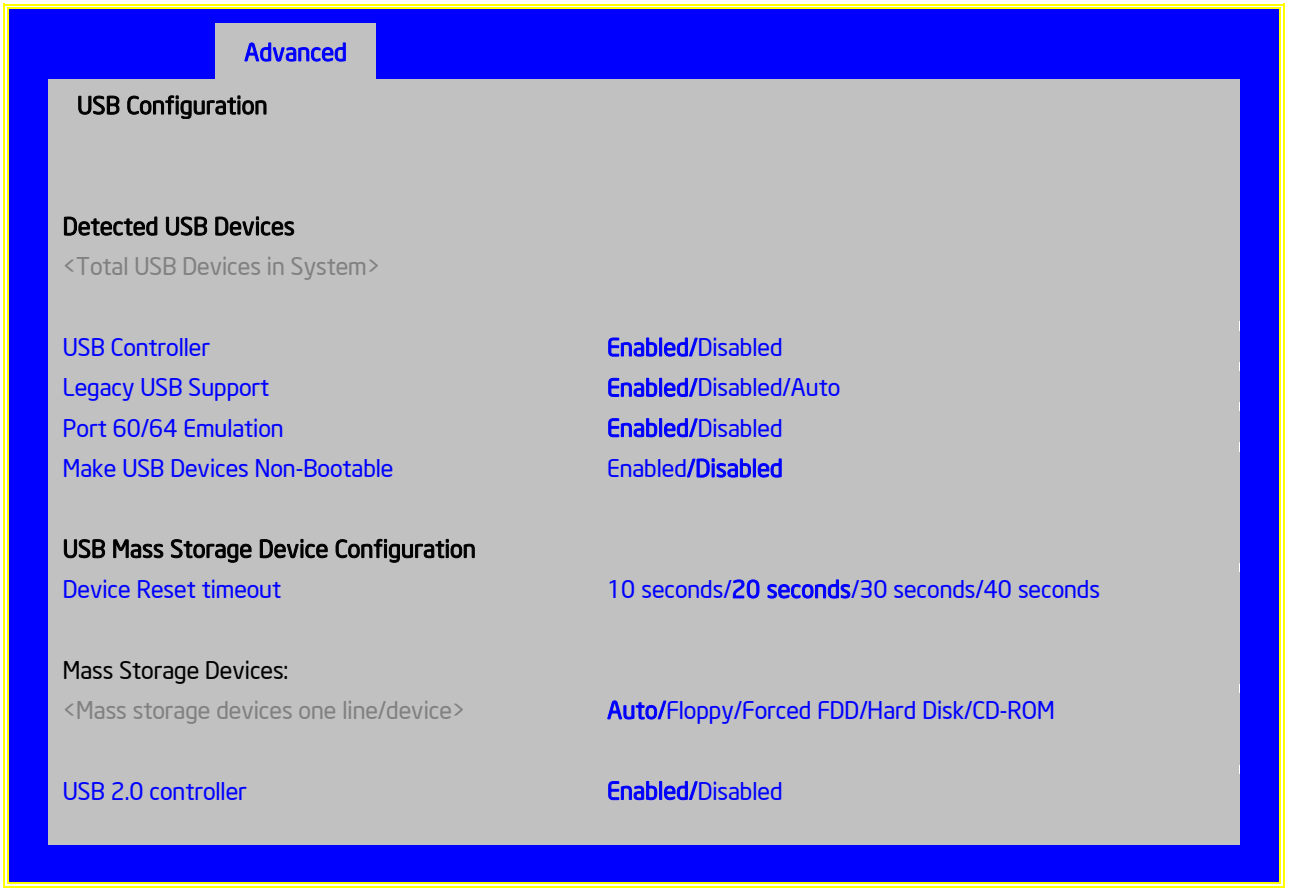


Figure 22. Setup Utility — USB Controller Configuration Screen Display

Table 23. 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, USB Devices Enabled displays the correct count, but can only display the first eight devices.
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**.

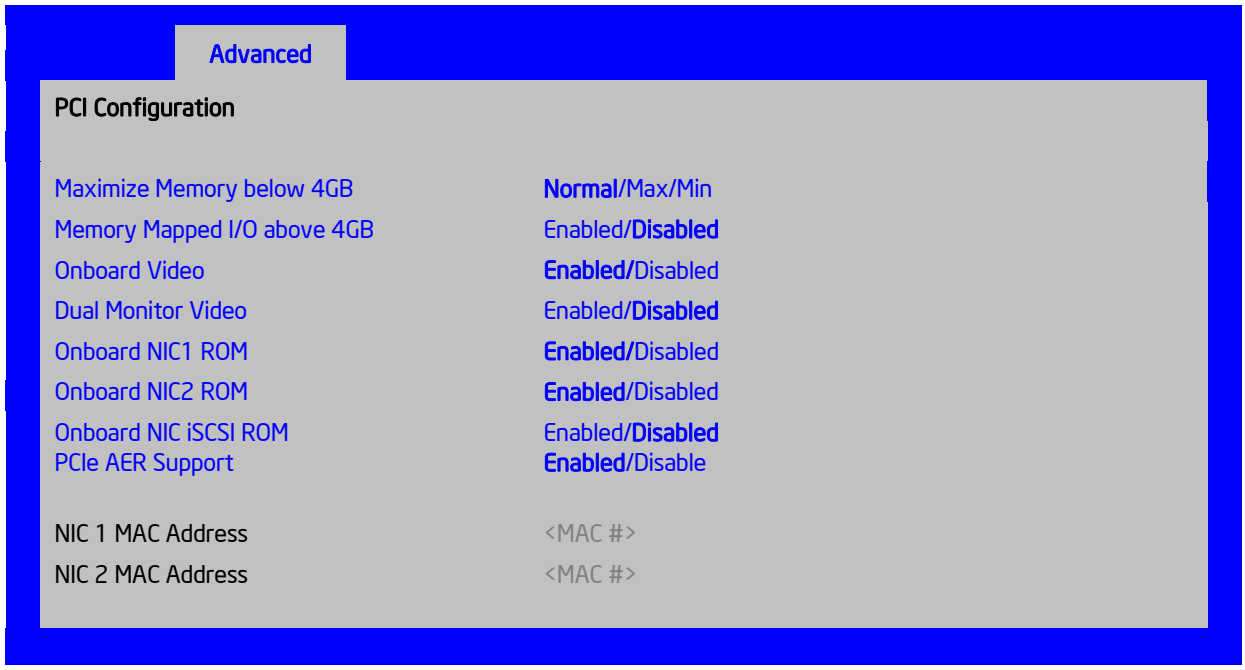


Figure 23. Setup Utility — PCI Configuration Screen Display

Table 24. Setup Utility — PCI Configuration Screen Fields

Setup Item	Options	Help Text	Comments
Maximize Memory below 4GB	Normal Max Min	BIOS maximize 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.	

Setup Item	Options	Help Text	Comments
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.	
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.
PCIe AER Support	Enable Disable	If enabled, BIOS allows OS control of PCIe AER (Advanced Error Reporting). In some cases, newer device drivers may be required in the OS. If disabled, BIOS disallows OS control of PCIe AER. BIOS will still log PCI error events in the SEL.	
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**.

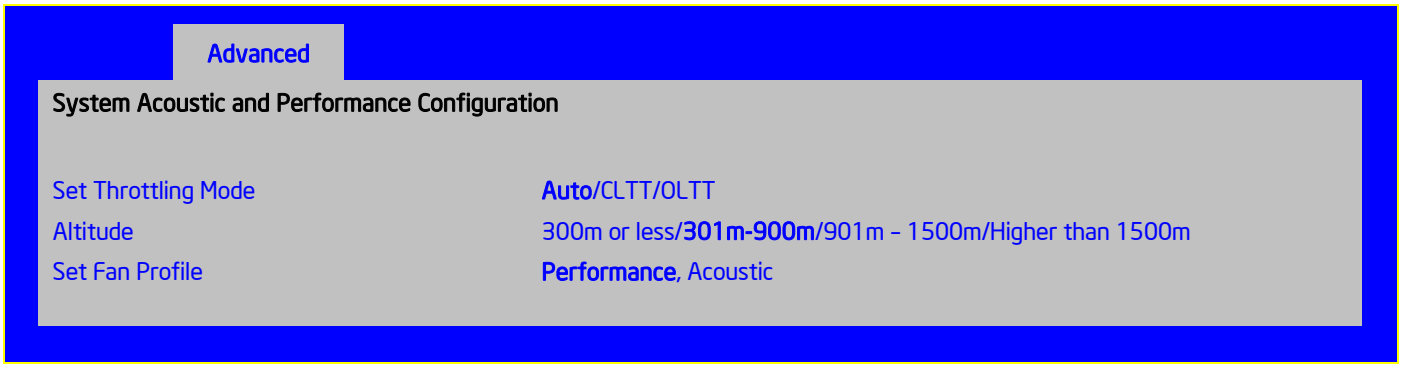


Figure 24. Setup Utility — System Acoustic and Performance Configuration Screen Display

Table 25. 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.	This option is hidden if CLTT is enabled.

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.

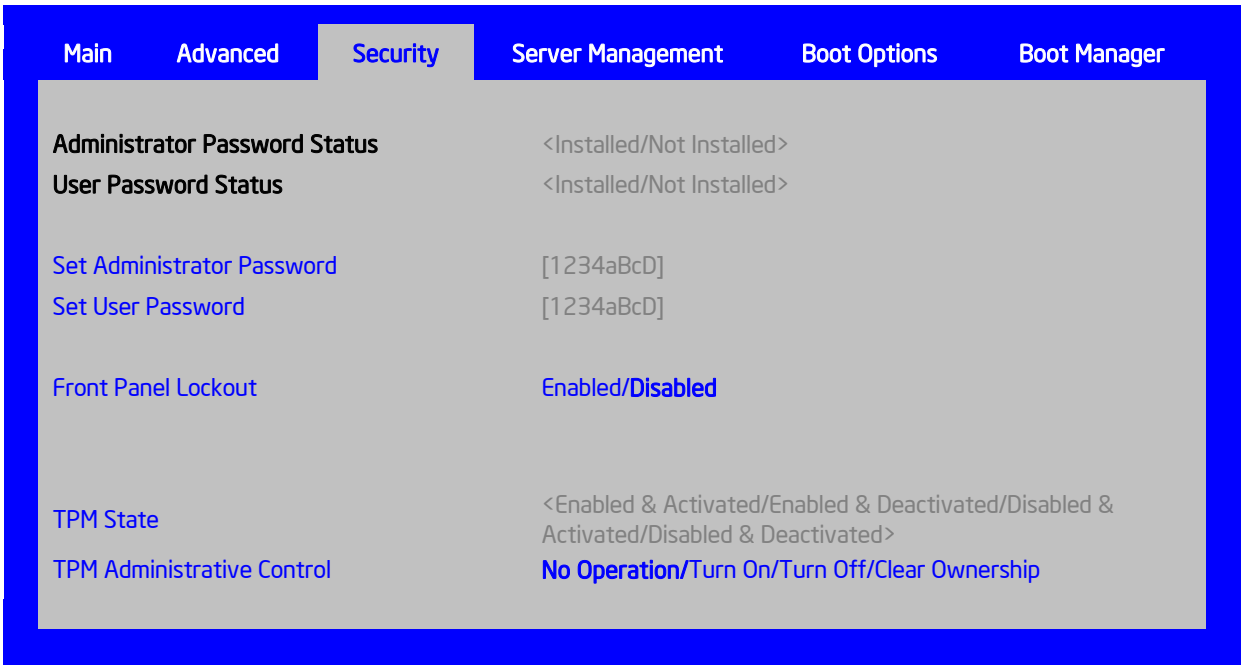


Figure 25. Setup Utility — Security Configuration Screen Display

Table 26. 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 only controls 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.

Setup Item	Options	Help Text	Comments
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.
TPM Administrative Control	No Operation Turn On Turn Off Clear Ownership	[No Operation] - No changes to current state. [Turn On] - Enables and activates TPM. [Turn Off] - Disables and deactivates TPM. [Clear Ownership] - Removes the TPM ownership authentication and returns the TPM to a factory default state. Note: The BIOS setting returns to [No Operation] on every boot cycle by default.	

5.3.2.4 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.

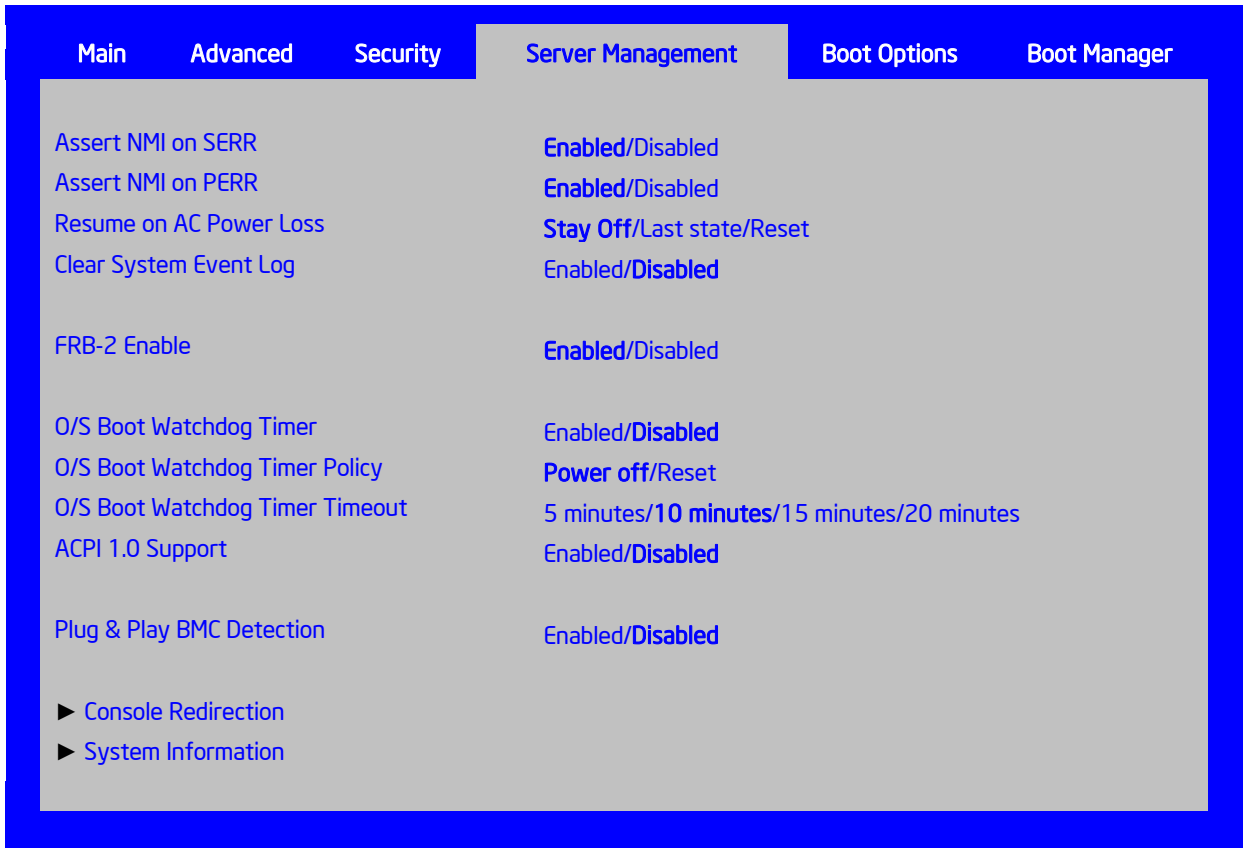


Figure 26. Setup Utility — Server Management Configuration Screen Display

Table 27. 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.	
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.

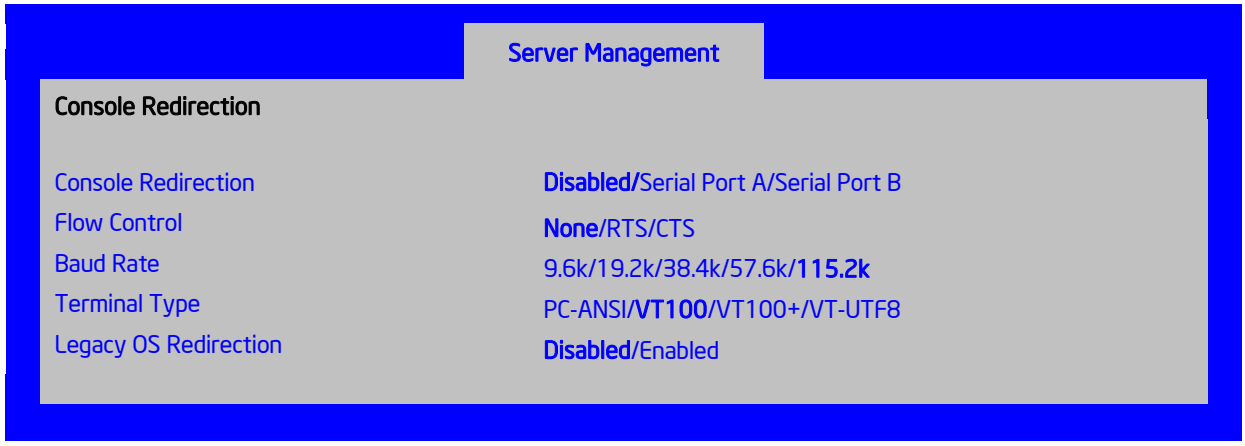


Figure 27. Setup Utility — Console Redirection Screen Display

Table 28. 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**.

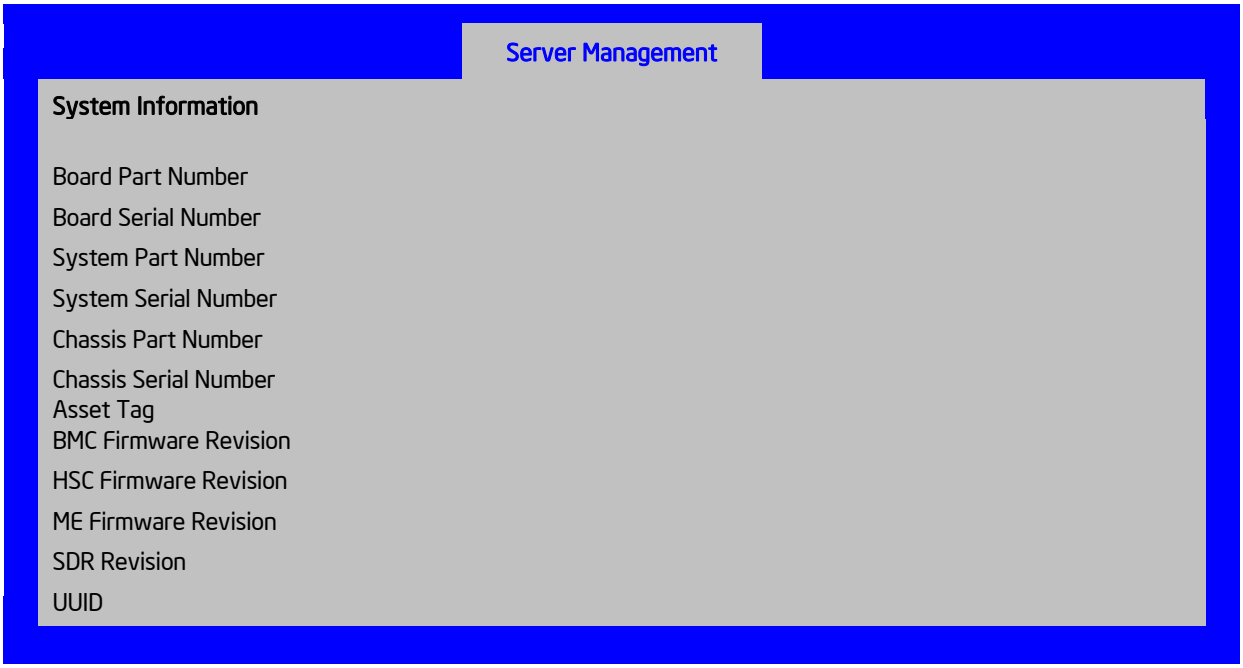


Figure 28. Setup Utility — Server Management System Information Screen Display

Table 29. 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 29. Setup Utility — Boot Options Screen Display

Table 30. 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	Set system boot order by selecting the boot	

Setup Item	Options	Help Text	Comments
	boot devices.	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 appears 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, 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**.

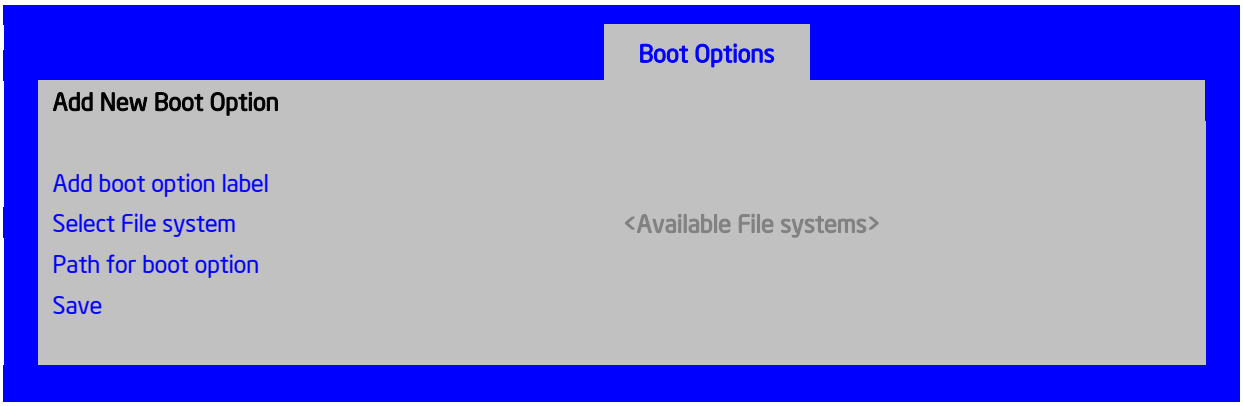


Figure 30. Setup Utility — Add New Boot Option Screen Display

Table 31. 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**.

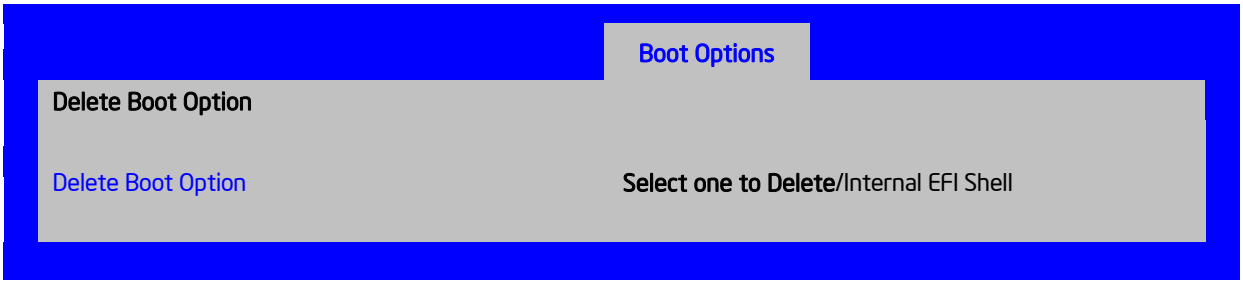


Figure 31. Setup Utility — Delete Boot Option Screen Display

Table 32. 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**.

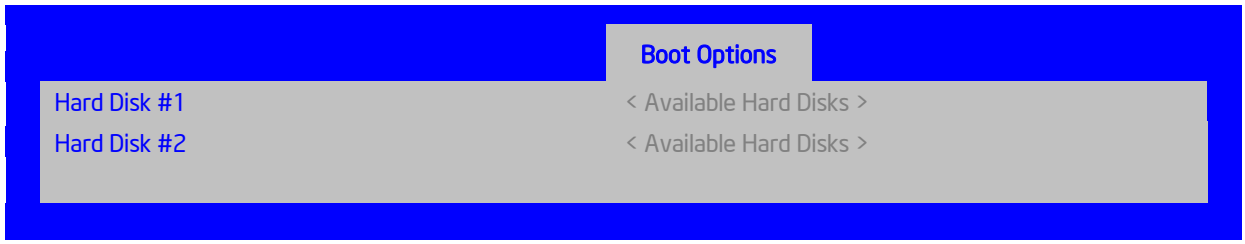


Figure 32. Setup Utility — Hard Disk Order Screen Display

Table 33. 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**.

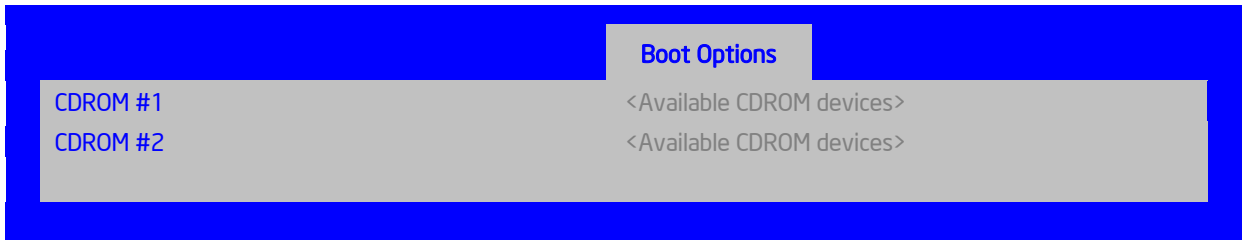


Figure 33. Setup Utility — CDROM Order Screen Display

Table 34. 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**.

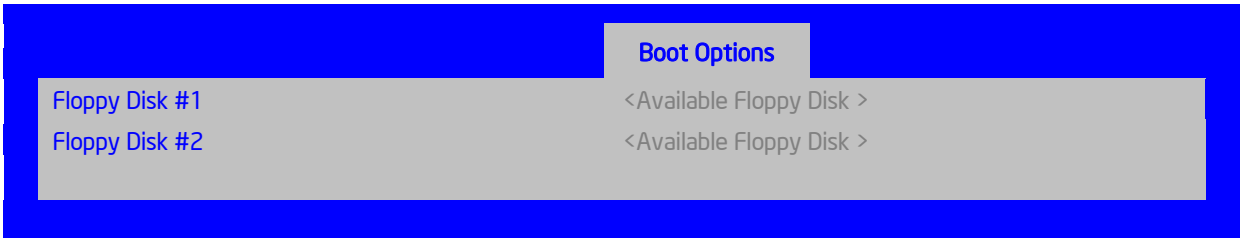


Figure 34. Setup Utility — Floppy Order Screen Display

Table 35. 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.
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**.

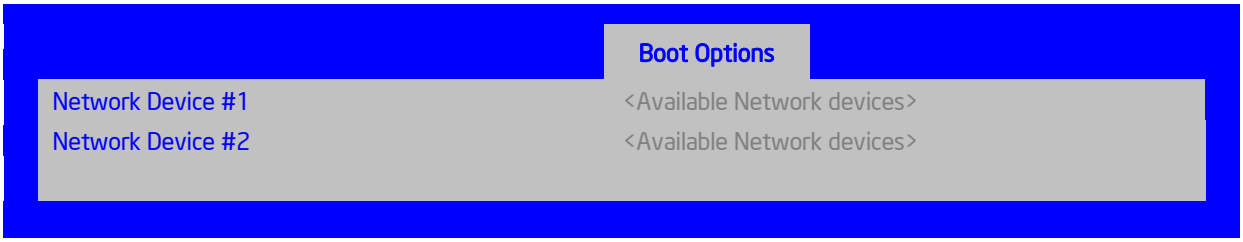


Figure 35. Setup Utility — Network Device Order Screen Display

Table 36. 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**.

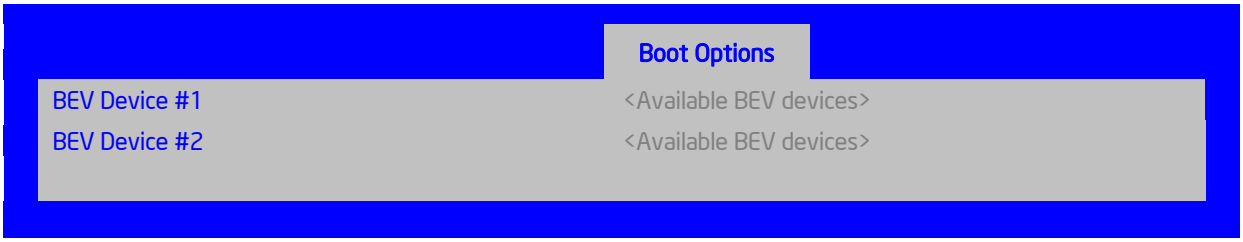


Figure 36. Setup Utility — BEV Device Order Screen Display

Table 37. 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.

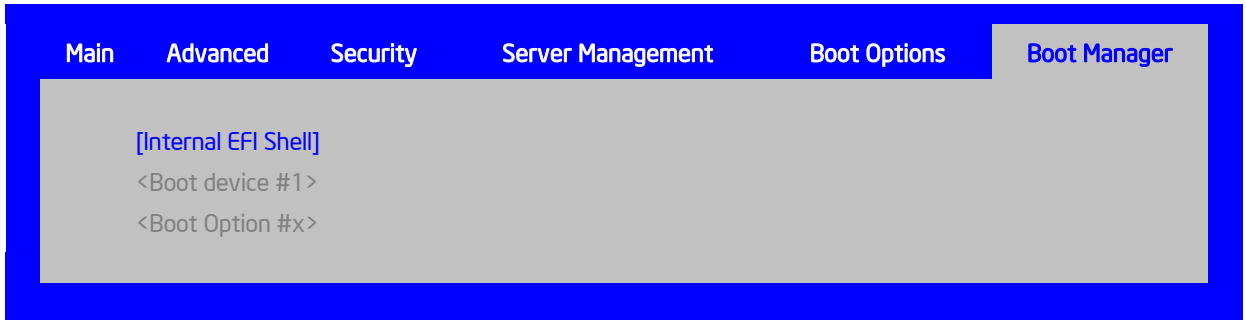


Figure 37. Setup Utility — Boot Manager Screen Display

Table 38. 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 38. Setup Utility — Error Manager Screen Display

Table 39. Setup Utility — Error Manager Screen Fields

Setup Item	Comments
Displays System Errors	Information only. Displays errors that occurred during the 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 set of user-defined default values. If Load Default Values is selected, the system applies the factory default settings (noted in bold in the tables in this chapter). If Load User Default Values is selected, the system is restored to the previously-saved, user-defined default values.

Figure 39. Setup Utility — Exit Screen Display

Table 40. 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 board. It lists all connector types available on the board and the corresponding reference designators printed on the silkscreen.

Table 41. Board Connector Matrix

Connector	Quantity	Reference Designators	Connector Type	Pin Count
Power supply	3	J2K1 J3K1 J1K2	Main power CPU 1 power P/S aux/IPMB	24 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 Riser	1	J4E1	Card edge	
Intel® RMM3	1	J5B1	Header	34
I/O Module	2	J3B1, J2B1	Mezzanine	50
SATA Software RAID Key	1	J1G6	Key holder	3
CPU Fans	2	J9K2, J9A4	Header	4
Memory Fans	2	J8K1, J9A3	Header	4
System Fans	2	J2J1, J2J3	Header	4
CPU fans	2	J7K1, J9A3	Header	4
Battery	1	BT4E1	Battery holder	3
RJ-45	2	J6A1, J6A2	External LAN	8
Stacked 2x USB	2	J7A1, J7A2	Dual USB	8
Video	1	J8A1	External DSub	15
Serial port A	1	J9A2	External RJ-45	9
Serial port B	1	J1A1	Header	9
Bridge board	1	J4H2	Header	
Fan board	1	J3J1	Header	
Front panel	1	J4H3	Header	24
Internal USB	1	J1J2	Header	10
Low-profile Internal USB for Intel® SSD	1	J1J1	Low-profile header	10
Chassis Intrusion	1	J1F4	Header	2
Serial ATA	6	J1G4, J1F3, J1F2, J1E3, J1E8, J1D6, J1D5	Header	7
SATA SGPIO	1	J1G5	Header	4
LCP/IPMB	1	J1H1	Header	4
Configuration jumpers	4	J1E7 (BIOS Default), J1E8 (Password Clear), J1D4 (BIOS Recovery), J1H2 (BMC Force Update)	Jumper	3

6.2 Power Connectors

The main power supply connection uses an SSI-compliant 2x12 pin connector (J2K1). In addition, there are three additional power related connectors:

- One SSI-compliant 2x4 pin power connector (J3K1), which provides 12 V power to the CPU Voltage Regulators and Memory.
- One SSI-compliant 1x5 pin connector (J1K2), which provides I^2C monitoring of the power supply.

The following tables define the connector pin-outs.

Table 42. Power Connector Pin-out (J2K1)

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 43. 12 V Power Connector Pin-out (J3K1)

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

Table 44. Power Supply Signal Connector Pin-out (J1K2)

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 (Intel® RMM3) Connector

A 34-pin Intel® RMM 3 connector (J5B1) is included on the server board to support the optional Intel® Remote Management Module 3. There is no support for third-party management cards on this server board.

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

Table 45. Intel® RMM3 Connector Pin-out (J5B1)

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)
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 server board and shorted to ground on the plug-in module)

6.3.2 LCP/IPMB Header

Table 46. LPC/IPMB Header Pin-out (J1H1)

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

6.3.3 SGPIO Header

Table 47. SGPIO Header Pin-out (J1G5)

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 SSI Control Panel Connector

The server board provides a 24-pin SSI front panel connector (J4H3) for use with Intel® and third-party chassis. The following table provides the pin-out for this connector.

Table 48. Front Panel SSI Standard 24-pin Connector Pin-out (J4H3)

Pin	Signal Name	Pin	Signal Name
1	P3V3_STBY (Power LED Anode)	2	P3V3_STBY (Front Panel Power)
3	Key	4	P5V_STBY (ID LED Anode)
5	FP_PWR_LED_N	6	FP_ID_LED_BUF_N
7	P3V3 (HDD Activity LED Anode)	8	FP_LED_STATUS_GREEN_N
9	LED_HDD_ACTIVITY_N	10	FP_LED_STATUS_A MBER_N
11	FP_PWR_BTN_N	12	NIC1_ACT_LED_N
13	GND (Power Button GND)	14	NIC1_LINK_LED_N
15	BMC_RST_BTN_N	16	SMB_SENSOR_3V3STB_DATA
17	GND (Reset GND)	18	SMB_SENSOR_3V3STB_CLK
19	FP_ID_BTN_N	20	FP_CHASSIS_INTRU
21	FM_SIO_TEMP_SENSOR	22	NIC2_ACT_LED_N
23	FP_NMI_BTN_N	24	NIC2_LINK_LED_N

Combined system BIOS and the Integrated BMC support provide the functionality of the various supported control panel buttons and LEDs. The following sections describe the supported functionality of each control panel feature.

Note: Control panel features are also routed through the bridge board connector at location J4G1, as is implemented in Intel® Server Systems configured using a bridge board and a hot-swap backplane.

6.4.1 Power Button

The BIOS supports a front control panel power button. Pressing the power button initiates a request that the Integrated BMC forwards to the ACPI power state machines in the chipset. It is monitored by the Integrated BMC and does not directly control power on the power supply.

- **Power Button — Off to On**
  The Integrated BMC monitors the power button and the wake-up event signals from the chipset. A transition from either source results in the Integrated BMC starting the power-up sequence. Since the processors are not executing, the BIOS does not participate in this sequence. The hardware receives the power good and reset signals from the Integrated BMC and then transitions to an ON state.
- **Power Button — On to Off (operating system absent)**
  The System Control Interrupt (SCI) is masked. The BIOS sets up the power button event to generate an SMI and checks the power button status bit in the ACPI hardware registers when an SMI occurs. If the status bit is set, the BIOS sets the ACPI power state of the machine in the chipset to the OFF state. The Integrated BMC monitors power state signals from the chipset and de-asserts PS_PWR_ON to the power supply. As a safety mechanism, the Integrated BMC automatically powers off the system in 4 to 5 seconds if the BIOS fails to service the request.
- **Power Button — On to Off (operating system present)**
  If an ACPI operating system is running, pressing the power button switch generates a request via SCI to the operating system to shut down the system. The operating system retains control of the system and the operating system policy determines the sleep state into which the system transitions, if any. Otherwise, the BIOS turns off the system.

6.4.2 Reset Button

The platform supports a front control panel reset button. Pressing the reset button initiates a request that is forwarded by the Integrated BMC to the chipset. The BIOS does not affect the behavior of the reset button.

6.4.3 NMI Button

The BIOS supports a front control panel NMI button. The NMI button may not be provided on all front panel designs. Pressing the NMI button initiates a request that causes the Integrated BMC to generate an NMI (non-maskable interrupt). The NMI is captured by the BIOS during boot services time, and by the operating system during runtime. During boot services time, the BIOS halts the system upon detection of the NMI.

6.4.4 Chassis Identify Button

The front panel chassis identify button toggles the state of the chassis ID LED. If the LED is off, pushing the ID button lights the LED. It remains lit until the button is pushed again or until a **Chassis Identify** or a **Chassis Identify LED** command is received to change the state of the LED.

6.4.5 Power LED

The green power LED is active when the system DC power is on. The power LED is controlled by the BIOS. The power LED reflects a combination of the state of system (DC) power and the system ACPI state. The following table identifies the different states that can be assumed by the power LED.

Table 49. Power LED Indicator States

State	ACPI	Power LED
Power off	No	Off
Power on	No	Solid on
S4/S5	Yes	Off
S1 Sleep	Yes	~1 Hz blink
S0	Yes	Solid on

6.4.6 System Status LED

Note: The system status LED state shows the state for the current, most severe fault. For example, if there was a critical fault due to one source and a non-critical fault due to another source, the system status LED state would be solid on (the state for the critical fault).

The system status LED is a bicolor LED. Green (status) is used to show a normal operation state or a degraded operation. Amber (fault) shows the system hardware state and overrides the green status.

The Integrated BMC-detected state and the state from other controllers, such as the SCSI/SATA hot-swap controller state, are included in the LED state. For fault states that are monitored by the Integrated BMC sensors, the contribution to the LED state follows the associated sensor state, with the priority going to the most critical state that is currently asserted.

When the server is powered down (transitions to the DC-off state or S5), the Integrated BMC is still on standby power and retains the sensor and front panel status LED state established prior to the power-down event.

The following table maps the system state to the LED state. For a complete list of events and their associated System Status, refer to the *Intel® Server System Integrated Baseboard Management Controller Core External Product Specification*.

Table 50. System Status LED Indicator States

Color	State	System Status	Description
Green	Solid on	Ok	System ready
Green	~1 Hz blink	Degraded	System degraded: BIOS detected 1. Unable to use all of the installed memory (more than one DIMM installed).[1] 2. In a mirrored configuration, when memory mirroring takes place and system loses memory redundancy. This is not covered by (2). [1] 3. PCI Express* correctable link errors. Integrated BMC detected 1. Redundancy loss such as power supply or fan. Applies only if the associated platform subsystem has redundancy capabilities. 2. CPU disabled – if there are two CPUs and one CPU is disabled. 3. Fan alarm – Fan failure. Number of operational fans should be more than minimum number needed to cool the system. 4. Non-critical threshold crossed – Temperature, voltage, power nozzle, power gauge, and PROCHOT[2] (Therm Ctrl) sensors. 5. Battery failure. 6. Predictive failure when the system has redundant power supplies.
Amber	~1 Hz blink	Non-Fatal	Non-fatal alarm – system is likely to fail: BIOS Detected 1. In non-mirroring mode, if the threshold of ten correctable errors is crossed within the window[1]. 2. PCI Express* uncorrectable link errors. Integrated BMC Detected 3. Critical threshold crossed – Voltage, temperature, power nozzle, power gauge, and PROCHOT (therm Ctrl) sensors. 4. VRD Hot asserted. 5. Minimum number of fans to cool the system are not present or have failed.

Color	State	System Status	Description
Amber	Solid on	Fatal	Fatal alarm – system has failed or shut down: BIOS Detected 1. DIMM failure when there is one DIMM present and no good memory is present[1]. 2. Run-time memory uncorrectable error in non-redundant mode[1]. 3. CPU configuration error (for instance, processor stepping mismatch). Integrated BMC Detected 1. CPU IERR signal asserted. 2. CPU 1 is missing. 3. CPU THERMTRIP. 4. No power good – power fault. 5. Power Unit Redundancy sensor – Insufficient resources offset (indicates not enough power supplies are present).
Off	N/A	Not ready	AC power off.

Notes:
1. The BIOS detects these conditions and sends a *Set Fault Indication* command to the Integrated BMC to provide the contribution to the system status LED.
2. Support for upper non-critical limit is not provided in default SDR configuration. However if a user does enable this threshold in the SDR, then the system status LED should behave as described.

6.4.7 Chassis ID LED

The chassis ID LED provides a visual indication of a system being serviced. The state of the chassis ID LED is affected by the following:

- Toggled by the chassis ID button
- Controlled by the *Chassis Identify* command (IPMI)
- Controlled by the *Chassis Identify LED* command (OEM)

Table 51. Chassis ID LED Indicator States

State	LED State
Identify active via button	Solid on
Identify active via command	~1 Hz blink
Off	Off

There is no precedence or lock-out mechanism for the control sources. When a new request arrives, all previous requests are terminated. For example, if the chassis ID LED is blinking and the chassis ID button is pressed, then the chassis ID LED changes to solid on. If the button is pressed again with no intervening commands, the chassis ID LED turns off.

6.5 Bridge Board Connector

For use in a supported Intel® Server Chassis, the server board provides a 120-pin high-density bridge board connector (J4H2) to route control panel, midplane, and backplane signals from the server board to the specified system board. The following table provides the pin-outs for this connector.

Table 52. 120-pin Bridge Board Connector Pin-out (J4H1)

Pin	Signal Name	Pin	Signal Name
A1	SMB_HOST_3V3_CLK	B1	GND
A2	SMB_HOST_3V3_DAT	B2	PE1_ESB_TXN_C<3>
A3	FM_BRIDGE_PRESENT_N	B3	PE1_ESB_TXP_C<3>
A4	GND	B4	GND
A5	PE1_ESB_RXN_C<3>	B5	PE_WAKE_N
A6	PE1_ESB_RXP_C<3>	B6	GND
A7	GND	B7	PE1_ESB_TXN_C<2>
A8	FM_FAN_D_PRSNT6	B8	PE1_ESB_TXP_C<2>
A9	GND	B9	GND
A10	PE1_ESB_RXN_C<2>	B10	FM_FAN_D_PRSNT5
A11	PE1_ESB_RXP_C<2>	B11	GND
A12	GND	B12	PE1_ESB_TXN_C<1>
A13	FM_FAN_D_PRSNT4	B13	PE1_ESB_TXP_C<1>
A14	GND	B14	GND
A15	PE1_ESB_RXN_C<1>	B15	RST_MP_PWRGD
A16	PE1_ESB_RXP_C<1>	B16	GND
A17	GND	B17	PE1_ESB_TXN_C<0>
A18	FM_RAID_PRESENT	B18	PE1_ESB_TXP_C<0>
A19	GND	B19	GND
A20	PE1_ESB_RXN_C<0>	B20	FM_RAID_MODE
A21	PE1_ESB_RXP_C<0>	B21	GND
A22	GND	B22	CLK_100M_SRLAKE_N
A23	FM_FAN_D_PRSNT1	B23	CLK_100M_SRLAKE_P
A24	FM_FAN_D_PRSNT3	B24	GND
A25	FM_FAN_D_PRSNT2	B25	SGPIO_DATAOUT1_R
A26	GND	B26	SGPIO_DATAOUT0_R
A27	USB_ESB_P4P	B27	SGPIO_LOAD_R
A28	USB_ESB_P4N	B28	SGPIO_CLOCK_N
A29	GND	B29	GND
A30	USB_ESB_OC_N<4>	B30	USB_ESB_P2P
A31	USB_ESB_OC_N<3>	B31	USB_ESB_P2N
A32	GND	B32	GND
A33	USB_ESB_P3P	B33	USB_ESB_OC_N<2>
A34	USB_ESB_P3N	B34	NIC1_LINK_LED_N
A35	GND	B35	NIC1_ACT_LED_N
A36	FP_NMI_BTN_N	B36	LED_STATUS_GREEN_R1
KEY		KEY	
A37	BMC_RST_BTN_N	B37	NIC2_LINK_LED_N
A38	FP_PWR_BTN_N	B38	NIC2_ACT_LED_N
A39	FP_ID_BTN	B39	LED_STATUS_AMBER_R1
A40	GND	B40	GND
A41	SMB_IPMB_ 5VSB_SDA	B41	SMB_SN_3V3SB_DAT_BUF
A42	SMB_IPMB_ 5VSB_CLK	B42	SMB_SN_3V3SB_CLK_BUF

Pin	Signal Name	Pin	Signal Name
A43	GND	B43	GND
A44	LED_ HDD_ACTIVITY_N	B44	V_IO_HSYNC2_BUF_FP
A45	P3V3	B45	V_IO_VSYNC2_BUF_FP
A46	FP_PWR_LED_N_R	B46	GND
A47	P3V3_STBY	B47	V_IO_BLUE_CONN_FP
A48	FP_ID_LED_R1_N	B48	V_IO_GREEN_CONN_FP
A49	FM_SIO_TEMP_SENSOR	B49	V_IO_RED_CONN_FP
A50	LED_FAN3_FAULT	B50	GND
A51	LED_FAN2_FAULT	B51	LED_FAN10_FAULT
A52	LED_FAN1_FAULT	B52	LED_FAN5_FAULT
A53	FAN_PWM_CPU1	B53	LED_FAN4_FAULT
A54	GND	B54	FAN_IO_PWM
A55	FAN_PWM_CPU2	B55	GND
A56	PCI_FAN_TACH9	B56	PCI_FAN_TACH10
A57	FAN_TACH7	B57	FAN_TACH8
A58	FAN_TACH5	B58	FAN_TACH6
A59	FAN_TACH3_H7	B59	FAN_TACH4_H7
A60	FAN_TACH1_H7	B60	FAN_TACH2_H7

6.6 I/O Connectors

6.6.1 VGA Connector

The following table details the pin-out definition of the VGA connector (J8A1).

Table 53. 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

6.6.2 NIC Connectors

The server board provides two stacked RJ-45/2xUSB connectors side-by-side on the back edge of the board (J6A1 and J6A2). The pin-out for NIC connectors are identical and are defined in the following table.

Table 54. RJ-45 10/100/1000 NIC Connector Pin-out (J6A1, J6A2)

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 (D1)	NIC_LINKA_1000_N (LED
12 (D2)	NIC_LINKA_100_N (LED)
13 (D3)	NIC_ACT_LED_N
14	NIC_LINK_LED_N
15	GND
16	GND

6.6.3 SATA/SAS Connectors

The server board provides up to six SATA/SAS connectors: SATA-0 (J1G4), SATA-1 (J1F3), SATA-2 (J1F2), SATA-3 (J1E3), SATA-4 (J1E8), and SATA-5 (J1D5).

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

Table 55. SATA/SAS Connector Pin-out (J1G5, J1F3, J1F2, J1E3, J1E8, J1D6, J1D5)

Pin	Signal Name	Description
1	GND	Ground
2	SATA/SAS_TX_P_C	Positive side of transmit differential pair
3	SATA/SAS_TX_N_C	Negative side of transmit differential pair
4	GND	Ground
5	SATA/SAS_RX_N_C	Negative side of receive differential pair
6	SATA/SAS_RX_P_C	Positive side of receive differential pair
7	GND	Ground

6.6.4 Intel® I/O Expansion Module Connector (J2B1, J3B1)

The server board provides 2x internal 50-pin mezzanine style connector (J2B1, J3B1) to accommodate proprietary form factor Intel® I/O Expansion Modules, which expand the IO capabilities of the server board without sacrificing an add-in slot from the riser cards. There are multiple IO modules for use on this server board. For more detail on the supported IO modules, refer to the *Intel® Server Board S5520UR*, S5520URT *IO Module Hardware Specification*. The following table details the pin-out of the Intel® I/O Expansion Module connectors.

Table 56. 50-pin Intel® I/O Expansion Module Connector Pin-out (J2B1, J3B1)

Pin	Signal Name	Pin	Signal Name
1	P3V3_AUX	2	P3V3_AUX
3	PE_RST_IO_MODULE_N	4	GND
5	GND	6	PE2_ESB_RXP_C<0>
7	GND	8	PE2_ESB_RXN_C<0>
9	PE2_ESB_TXP_C<0>	10	GND
11	PE2_ESB_TXN_C<0>	12	GND
13	GND	14	PE2_ESB_RXP_C<1>
15	GND	16	PE2_ESB_RXN_C<1>
17	PE2_ESB_TXP_C<1>	18	GND
19	PE2_ESB_TXN_C<1>	20	GND
21	GND	22	PE2_ESB_RXP_C<2>
22	GND	24	PE2_ESB_RXN_C<2>
25	PE2_ESB_TXP_C<2>	26	GND
27	PE2_ESB_TXN_C<2>	28	GND
29	GND	30	PE2_ESB_RXP_C<3>
31	GND	32	PE2_ESB_RXN_C<3>
33	PE2_ESB_TXP_C<3>	34	GND
35	PE2_ESB_TXN_C<3>	36	GND
37	GND	38	CLK_100M_LP_PCIE_SLOT3_P
39	GND	40	CLK_100M_LP_PCIE_SLOT3_N
41	PE_WAKE_N	42	GND
43	P3V3	44	P3V3
45	P3V3	46	P3V3
47	P3V3	48	P3V3
49	P3V3	50	P3V3

6.6.5 Serial Port Connectors

The server board provides one external RJ-45 Serial A port (J9A2) and one internal 9-pin serial B header (J1A1). The following tables define the pin-outs.

Table 57. External RJ-45 Serial A Port Pin-out (J9A2)

Pin	Signal Name	Description
1	SPB_RTS	RTS (request to send)
2	SPB_DTR	DTR (Data terminal ready)
3	SPB_OUT_N	TXD (Transmit data)
4	GND	Ground
5	SPB_RI	RI (Ring Indicate)
6	SPB_SIN_N	RXD (receive data)
7	SPB_DSR _DCD	Data Set Ready/Data Carrier Detect
8	SPB_CTS	CTS (clear to send)

Table 58. Internal 9-pin Serial B Header Pin-out (J1A1)

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

6.6.6 USB Connector

The following table details the pin-out of the external USB connectors (J7A1 and J7A2) found on the back edge of the server board.

Table 59. External USB Connector Pin-out (J7A1, J7A2)

Pin	Signal Name	Description
1	USB_OC	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

One 2x5 connector on the server board (J1J2) provides an option to support additional two USB ports. The pin-out of the connector is detailed in the following table:

Table 60. Internal USB Connector Pin-out (J1J2)

Pin	Signal Name	Description
1	USB2_VBUS4	USB power (port 4)
2	USB2_VBUS5	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

One low-profile 2x5 connectors (J1D1) on the server board provides an option to support low-profile Intel® Z-U130 Value Solid State Drive. The pin-out of the connector is detailed in the following table.

Table 61. Pin-out of Internal USB Connector for low-profile Intel® Z-U130 Value Solid State Drive (J1D1)

Pin	Signal Name	Description
1	+5V	USB power
2	NC	
3	USB Data -	USB port negative signal
4	NC	
5	USB Data +	USB port positive signal
6	NC	
7	Ground	
8	NC	
9	Key	No pin
10	LED#	Activity LED

6.7 Riser Card Slot

The server board has one riser slot, utilizing Intel® Adaptive Slot Technology, which serves both full-height and half-height cards with PCI-X and/or PCI-Express* interface depending on chassis configuration.

Note: The PCI-X interface is supported using 2U Butterfly PCI Express*/PCI-X active riser.

The riser connector is a 280-pin PCI Express* connector from FCI-Berg (Vendor P/N: 10027747-11110TLF). The pin-out defines four Power Rails (3.3V, 3.3VAUX, 5V, 12V, and N12V), 24 lanes of PCI Express* Gen2 lanes, seven Reference Clocks along with various sideband signals. One RSVD pin is strapped to the ground on the server board and is not used on the Riser.

The pin-out defines the PCI Express* signals in two ways:

- TP[x] and TN[x] are the generic signal names indicating the Transmit pairs; RP[x] and RN[x] are the generic signal names indicating the Receive pairs.
- PEx_Tx[x] and PEx_Rx[x] are the actual signal names used in the design.

Table 62. Pin-out of adaptive riser slot

Pin Side B	PCI Express* Signal	PCI Express* Signal	Pin Side A	Pin Side B	PCI Express* Signal	PCI Express* Signal	Pin Side A
1	3.3V	3.3V	1	70	GND	RP[6] { PE5_Rp [1] }	70
2	3.3V	3.3V	2	71	GND	RN[6] { PE5_Rn [1] }	71
3	GND	3.3V	3	72	TP[5] { PE5_Tp [2] }	GND	72
4	GND	3.3V	4	73	TN[5] { PE5_Tn [2] }	GND	73
5	GND	3.3V	5	74	GND	RP[5] { PE5_Rn [2] }	74
6	GND	3.3V	6	75	GND	RN[5] { PE5_Rp [2] }	75
7	GND	3.3V	7	76	TP[4] { PE5_Tp [3] }	GND	76
8	GND	3.3V	8	77	TN[4] { PE5_Tn [3] }	GND	77
9	GND	3.3V	9	78	GND	RP[4] { PE5_Rp [3] }	78
10	3.3V	3.3V	10	79	GND	RN[4] { PE5_Rn [3] }	79
11	3.3V	3.3V	11	80	TP[3] { PE6_Tp [0] }	GND	80
KEY	KEY	KEY	KEY	81	TN[3] { PE6_Tn [0] }	GND	81
KEY	KEY	KEY	KEY	82	GND	RP[3] { PE6_Rn [0] }	82
12	GND	3.3V	12	83	GND	RN[3] { PE6_Rp [0] }	83
13	GND	3.3V	13	84	TP[2] { PE6_Tp [1] }	GND	84
14	3.3VAUX	3.3V	14	85	TN[2] { PE6_Tn [1] }	GND	85
15	3.3VAUX	3.3V	15	86	GND	RP[2] { PE6_Rp [1] }	86
16	GND	12V	16	87	GND	RN[2] { PE6_Rn [1] }	87
17	GND	12V	17	88	TP[1] { PE6_Tn [2] }	GND	88
18	GND	12V	18	89	TN[1] { PE6_Tp [2] }	GND	89
19	GND	12V	19	90	GND	RP[1] { PE6_Rn [2] }	90
20	GND	12V	20	91	GND	RN[1] { PE6_Rp [2] }	91
21	GND	12V	21	92	TP[0] { PE6_Tp [3] }	GND	92

Pin Side B	PCI Express* Signal	PCI Express* Signal	Pin Side A
22	N12V	12V	22
23	PME#	12V	23
24	PERST#	5V	24
25	GND	5V	25
26	GND	5V	26
27	GND	5V	27
28	GND	5V	28
29	Riser Type [0]	WAKE#	29
30	Riser Type [1]	CHASSIS INTRUSION	30
31	GND	RSVD	31
32	TP[7] { PE3_Tp [0] }	GND	32
33	TN[7] { PE3_Tn [0] }	GND	33
34	GND	RP[7] { PE3_Rp [0] }	34
35	GND	RN[7] { PE3_Rn [0] }	35
36	TP[6] { PE3_Tn [1] }	GND	36
37	TN[6] { PE3_Tp [1] }	GND	37
38	GND	RP[6] { PE3_Rn [1] }	38
39	GND	RN[6] { PE3_Rp [1] }	39
40	TP[5] { PE3_Tp [2] }	GND	40
41	TN[5] { PE3_Tn [2] }	GND	41
42	GND	RP[5] { PE3_Rn [2] }	42
43	GND	RN[5] { PE3_Rp [2] }	43
44	TP[4] { PE3_Tp [3] }	GND	44
45	TN[4] { PE3_Tn [3] }	GND	45
46	GND	RP[4] { PE3_Rp [3] }	46
47	GND	RN[4] { PE3_Rn [3] }	47
48	TP[3] { PE4_Tn [0] }	GND	48
49	TN[3] { PE4_Tp [0] }	GND	49
50	GND	RP[3] { PE4_Rp [0] }	50
51	GND	RN[3] { PE4_Rn [0] }	51
52	TP[2] { PE4_Tn [1] }	GND	52
53	TN[2] { PE4_Tp [1] }	GND	53
54	GND	RP[2] { PE4_Rp [1] }	54
55	GND	RN[2] { PE4_Rn [1] }	55
56	TP[1] { PE4_Tn [2] }	GND	56
57	TN[1] { PE4_Tp [2] }	GND	57
58	GND	RP[1] { PE4_Rp [2] }	58
59	GND	RN[1] { PE4_Rn [2] }	59
60	TP[0] { PE4_Tp [3] }	GND	60
61	TN[0] { PE4_Tn [3] }	GND	61
62	GND	RP[0] { PE4_Rn [3] }	62
63	GND	RN[0] { PE4_Rp [3] }	63
64	TP[7] { PE5_Tn [0] }	GND	64
65	TN[7] { PE5_Tp [0] }	GND	65
66	GND	RP[7] { PE5_Rn [0] }	66

Pin Side B	PCI Express* Signal	PCI Express* Signal	Pin Side A
93	TN[0] { PE6_Tn [3] }	GND	93
94	GND	RP[0] { PE6_Rn [3] }	94
95	GND	RN[0] { PE6_Rp [3] }	95
96	TP[7] { PE7_Tp [0] }	GND	96
97	TN[7] { PE7_Tn [0] }	GND	97
98	GND	RP[7] { PE7_Rn [0] }	98
99	GND	RN[7] { PE7_Rp [0] }	99
100	TP[6] { PE7_Tn [1] }	GND	100
101	TN[6] { PE7_Tp [1] }	GND	101
102	GND	RP[6] { PE7_Rp [1] }	102
103	GND	RN[6] { PE7_Rn [1] }	103
104	TP[5] { PE7_Tp [2] }	GND	104
105	TN[5] { PE7_Tn [2] }	GND	105
106	GND	RP[5] { PE7_Rp [2] }	106
107	GND	RN[5] { PE7_Rn [2] }	107
108	TP[4] { PE7_Tn [3] }	GND	108
109	TN[4] { PE7_Tp [3] }	GND	109
110	GND	RP[4] { PE7_Rp [3] }	110
111	GND	RN[4] { PE7_Rn [3] }	111
112	TP[3] { PE8_Tn [0] }	GND	112
113	TN[3] { PE8_Tp [0] }	GND	113
114	GND	RP[3] { PE8_Rn [0] }	114
115	GND	RN[3] { PE8_Rp [0] }	115
116	TP[2] { PE8_Tp [1] }	GND	116
117	TN[2] { PE8_Tn [1] }	GND	117
118	GND	RP[2] { PE8_Rp [1] }	118
119	GND	RN[2] { PE8_Rn [1] }	119
120	TP[1] { PE8_Tp [2] }	GND	120
121	TN[1] { PE8_Tn [2] }	GND	121
122	GND	RP[1] { PE8_Rp [2] }	122
123	GND	RN[1] { PE8_Rn [2] }	123
124	TP[0] { PE8_Tp [3] }	GND	124
125	TN[0] { PE8_Tn [3] }	GND	125
126	GND	RP[0] { PE8_Rn [3] }	126
127	GND	RN[0] { PE8_Rp [3] }	127
128	REFCLK+ [1]	GND	128
129	REFCLK- [1]	GND	129
130	GND	REFCLK+ [2]	130
131	GND	REFCLK- [2]	131
132	REFCLK+ [3]	GND	132
133	REFCLK- [3]	GND	133
134	GND	REFCLK+ [4]	134
135	REFCLK+ [5]	REFCLK- [4]	135
136	REFCLK- [5]	GND	136
137	GND	REFCLK+ [6]	137

Pin Side B	PCI Express* Signal	PCI Express* Signal	Pin Side A
67	GND	RN[7] { PE5_Rp [0] }	67
68	TP[6] { PE5_Tn [1] }	GND	68
69	TN[6] { PE5_Tp [1] }	GND	69

Pin Side B	PCI Express* Signal	PCI Express* Signal	Pin Side A
138	REFCLK+ [7]	REFCLK- [6]	138
139	REFCLK- [7]	GND	139
140	Riser Type [3]	Riser Type [2]	140

Table 63. Pin Type Description

Pin Types	Description
3.3 V	3.3 V Power Rail
12 V	12 V Power Rail
N12 V	Negative 12 V Power Rail
3.3VAUX	3.3 V AUX Rail
5 V	5 V Power Rail for PCI-X
PE	PCI Express* Gen2 Signals
SMBus	SMBus Signals have been removed; No SW support
MISC	WAKE#, PERST#, CH INTR, PME#
JTAG	These have been removed
CLKS	Clocks
Riser Type	Riser Type Signals
RSVD	Reserved Pins

6.7.1 PCI Express* Port Bifurcation

The IOH supports various combinations of link sizes ranging from x2 to x16 through bifurcation of PCI Express* ports. However, the ports that can be combined to form larger links are limited. You cannot combine any ports to form a larger link. The following table details how the ports can be combined.

Table 64. PCI Express* Port Bifurcation

Intel® ICH10	Signal Type	Signal Name	Description
PE1	PE1RN[3:0], PE1RP[3:0], PE1TN[3:0], PE1TP[3:0]	x4	
PE2	PE2RN[3:0], PE2RP[3:0], PE2TN[3:0], PE2TP[3:0]		
PE3	PE3RN[3:0], PE3RP[3:0], PE3TN[3:0], PE3TP[3:0]	X8	X16
PE4	PE4RN[3:0], PE4RP[3:0], PE4TN[3:0], PE4TP[3:0]		
PE5	PE5RN[3:0], PE5RP[3:0], PE5TN[3:0], PE5TP[3:0]	X8	
PE6	PE6RN[3:0], PE6RP[3:0], PE6TN[3:0], PE6TP[3:0]		
PE7	PE7RN[3:0], PE7RP[3:0], PE7TN[3:0], PE7TP[3:0]	X8	X16
PE8	PE8RN[1:0], PE8RP[1:0], PE8TN[1:0], PE8TP[1:0]		
PE9	PE9RN[1:0], PE9RP[1:0], PE9TN[1:0], PE9TP[1:0]	X8	
PE10	PE10RN[1:0], PE10RP[1:0], PE10TN[1:0], PE10TP[1:0]		
DMI	DMIRN[3:0], DMIRP[3:0], DMITN[3:0], DMITP[3:0]	Not Combinable	
Common Signals	PE{0/1}CLKN, PE{0/1}CLKP, VCCAPE, VSS, PE{0/1}ICOMPI, PE{0/1}RCOMPO, VCCAPEBG, VSSAPEBG	Common Signals	

6.7.2 'Riser Type' Signals

The riser connector pin-out contains four Riser Type (or Riser ID) pins. These signals are part of the IOH's PEWIDTH bits that are strapping options for configuring the PCI Express* ports at system power-on. Each of the Intel® Server System SR2600/SR2625/SR1600/SR1625 risers has been optimally defined to strap the PEWIDTH bits through the Riser Type pins to either eliminate or reduce the need for software configurations of the PCI Express* ports.

IOH's PEWIDTH contains a total of six bits. The acceptable values of PEWIDTH ranges from PEWIDTH[5:0] = 00_0000b to PEWIDTH[5:0] = 11_1011b. For a description of how PEWIDTH configures the PCI Express* lanes, refer to the *Intel® 5500/5520 Chipset I/O Hub (IOH) External Design Specification*. A subset of the supported values and resulting configuration is shown in the following table.

Table 65. Port Bifurcation Control

PEWIDTH[5:0]	Port1	Port2	Port3	Port4	Port5	Port6	Port7	Port8	Port9	Port10
11111	Wait-on-BIOS									
100000	x4	Not present	x4	x4	X4	x4	x4	x4	x4	x4
100001	x4	Not present	x4	x4	X4	x4	x8	Not present	x4	x4
100010	x4	Not present	x4	x4	X4	x4	x4	x4	x8	Not present
100011	x4	Not present	x4	x4	X4	x4	X8	Not present	x8	Not present
100100	x4	Not present	x8	Not present	X4	x4	x4	x4	x4	x4
100101	x4	Not present	x8	Not present	X4	x4	X8	Not present	x4	x4
100110	x4	Not present	x8	Not present	X4	x4	x4	x4	x8	Not present
100111	x4	Not present	x8	Not present	X4	x4	X8	Not present	x8	Not present
101000	x4	Not present	x4	x4	X8	Not present	x4	x4	x4	x4
101001	x4	Not present	x4	x4	X8	Not present	X8	Not present	x4	x4
101010	x4	Not present	x4	x4	X8	Not present	x4	x4	x8	Not present
101011	x4	Not present	x4	x4	X8	Not present	X8	Not present	x8	Not present
101100	x4	Not present	x8	Not present	X8	Not present	x4	x4	x4	x4
101101	x4	Not present	x8	Not present	X8	Not present	X8	Not present	x4	x4
101110	x4	Not present	x8	Not present	X8	Not present	x4	x4	x8	Not present
101111	x4	Not present	x8	Not present	X8	Not present	X8	Not present	x8	Not present
110000	x4	Not present	x16	Not present	Not present	Not present	x4	x4	x4	x4
110001	x4	Not present	x16	Not present	Not present	Not present	X8	Not present	x4	x4
110010	x4	Not present	x16	Not present	Not present	Not present	x4	x4	x8	Not present
110011	x4	Not present	x16	Not present	Not present	Not present	X8	Not present	x8	Not present

See Table 9 in Section 3.4.1 for the port mapping on Intel® Server Board S5520UR , S5520URT

Although the PEWIDTH contains a total of six bits, only four are routed to the riser. The following table shows the mapping of RiserType[3:0] pins to PEWIDTH[5:0].

Table 66. RiserType and PEWIDTH Mapping

IOH Strapping	PEWIDTH[5]	PEWIDTH[4]	PEWIDTH[3]	PEWIDTH[2]	PEWIDTH[1]	PEWIDTH[0]
Riser/Server board	(Server board)	RiserType[3]	RiserType[2]	RiserType[1]	(Server board)	RiserType[0]

PEWIDTH[5] is pulled high by the server board while PEWIDTH[1] is controlled by the I/O expansion module.

6.7.2.1 Strapping Option

Intel® Server Board S5520UR, S5520URT risers support a pull-down resistor strapping option for each of the four RiserType pins. The pull-up resistors are not required on the riser as they are located on the server board. A strong resistor value of 100 ohms or less is recommended on the riser.

6.7.3 PCI Express* Trace Length Consideration

PCI Express* Gen2 lanes have a maximum trace length requirement that is considerably shorter than for Gen1. Given the significant differences in trace lengths on the server board, Intel® Server Board S5520UR, S5520URT risers have the IOH port assigned to the PCI Express* slot that minimizes any one lane going beyond the maximum trace length specification.

The following table provides the trace lengths from the IOH to the riser slot. Given that the trace length varies from a minimum of 4.5 inches to maximum of 7.8 inches on the server board, traces on any riser card need to be routed to keep the maximum length under the specification.

Table 67. Trace Lengths

Server board (IOH)	Netnames	Length (inches)
PE3	P2E_IOH_SLOT**6**_[7:4]	4.5
PE4	P2E_IOH_SLOT**6**_[3:0]	5.0
PE5	P2E_IOH_SLOT**5**_[7:4]	5.7
PE6	P2E_IOH_SLOT**5**_[3:0]	6.7
PE7	P2E_IOH_SLOT**4**_[7:4]	7.4
PE8	P2E_IOH_SLOT**4**_[3:0]	7.8

6.7.4 Reference Clocks

Seven 100-MHz reference clocks are provided to the riser from the DB1200 Clock Buffer on the server board. These clocks can be used for PCI Express* slots or various devices such as PCI Express* packet switches and PCI Express* to PCI-X bridges. As these clocks are kept enabled by default, there are no rules for assigning the IOH PCI Express* port to Clock to Slot. Any of the clocks can be used in the design.

6.7.5 Power Budget

The Power Rail pins have been defined with the maximum current per rail as mentioned in the following table.

Table 68. Power Budget

	Power Rails				
	3.3V	5V	12V	3.3VAUX	N12V
Max Current Per Rail (A)	17.7	5	7.3	1	1

It's important to note that the above "Board-Level" power budget does not take into account the limitations placed at the "System-Level" power budget. The above current numbers should only be understood as the maximum current limit that the design can handle. The riser and server board in the system must comply with any System-Level limitations that are typically set due to thermal concerns.

6.7.6 Decoupling

Decoupling caps must be added on the riser as per the PCI Express Specification for all Power Rails used on the riser.

6.7.7 Mechanical Considerations for Intel® Chassis

There are various mechanical considerations that must be followed when designing for an Intel® Server Chassis. Use the mechanical control drawings of the 1U and 2U Intel®-designed risers as reference for any custom designs.

6.8 Fan Headers

The server board provides six SSI-compliant 4-pin fan headers to be used as CPU, and I/O cooling fans in non-Intel® chassis. 3-pin and 4-pin fans are supported on all fan headers. The pin configuration for each of the 4-pin fan headers is identical and is defined in the following table.

- CPU1 fan (J9A4)
- CPU2 fan (J9K2)
- MEM1 fan (J8K1)
- MEM2 fan (J9A3)
- SYS1 fan (J3J2)
- SYS2 fan (J3J1)

Table 69. SSI 4-pin Fan Header Pin-out (J9A4, J9K2, J8K1, J9A3, J3J2, and J3J1)

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

When the server board is integrated into an Intel® Server System with fixed hard drives, system fan monitoring is supported through a custom 26-pin connector with the pin-out defined in the following table.

Table 70. Server Board-to-System Fan Board Connector Pin-out (Intel® Chassis Only)

Pin Definition	Pin #		Pin Definition
FAN_PWM_CPU1	1	2	FAN_PWM_CPU2
FM_FAN_D_PRSNT1_N	3	4	FAN_IO_PWM
FM_FAN_D_PRSNT3_N	5	6	FM_FAN_D_PRSNT2_N
FM_FAN_D_PRSNT5_N	7	8	FM_FAN_D_PRSNT4_N
Empty – Connector Key	9	10	LED_FAN1_FAULT
LED_FAN2_FAULT	11	12	LED_FAN3_FAULT
LED_FAN4_FAULT	13	14	LED_FAN5_FAULT
FAN_TACH1_H7	15	16	FAN_TACH2_H7
FAN_TACH3_H7	17	18	FAN_TACH4_H7
FAN_TACH5	19	20	FAN_TACH6
FAN_TACH7	21	22	FAN_TACH8
PCI_FAN_TACH9	23	24	CONN_PIN24_R
PCI_FAN_TACH10	25	26	FM_SIO_TEMP_SENSOR

Note: Intel Corporation server boards support peripheral components and 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 their published operating or non-operating limits.

7. Jumper Blocks

The server board has several 3-pin jumper blocks that can be used to configure, protect, or recover specific features of the server board.

Pin 1 on each jumper block can be identified by the following symbol on the silkscreen: ▼

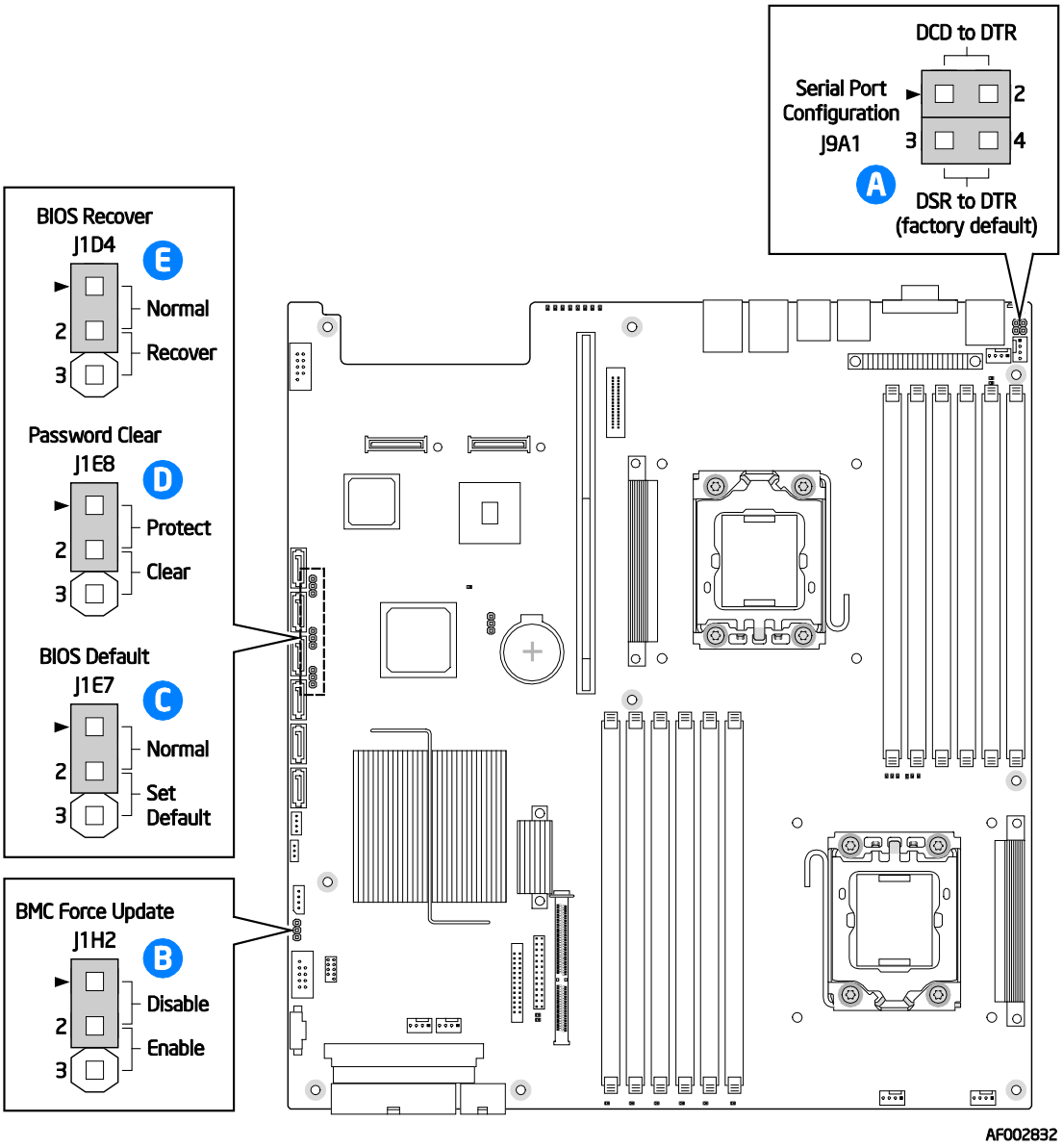


Figure 40. Jumper Blocks (J1C3, J1D1, J1D2, J1E32)

Table 71. Server Board Jumpers (J1E7, J1E8, J1D4, and J1H2)

Jumper Name	Pins	System Results
J1E7: BIOS Default	1-2	These pins should have a jumper in place for normal system operation. **(Default)**
	2-3	If these pins are jumpered with AC power plugged, the BIOS settings are cleared within 5 seconds. These pins should not be jumpered for normal operation.
J1E8: Password Clear	1-2	These pins should have a jumper in place for normal system operation. **(Default)**
	2-3	If these pins are jumpered, administrator and user passwords are cleared within 5-10 seconds after the system is powered on. These pins should not be jumpered for normal operation.
J1D4: BIOS Recover	1-2	These pins should have a jumper in place for normal system operation. **(Default)**
	2-3	Given that the main system BIOS will not boot with these pins jumpered, system can only boot from EFI-bootable recovery media with the recovery BIOS image.
J1H2: BMC Force Update	1-2	Integrated BMC Firmware Force Update Mode – Disabled **(Default)**
	2-3	Integrated BMC Firmware Force Update Mode – Enabled

7.1 BIOS Defaults and Password Clear Usage Procedure

The BIOS Default (J1E7) and Password Clear (J1E8) recovery features are designed such that the desired operation can be achieved with minimal system downtime. 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 Restoring BIOS Defaults

To restore BIOS Defaults, perform the following steps:

1. Power down the server. Do not unplug the power cord.
2. Open the server chassis. For instructions, see your server chassis documentation.
3. Move jumper (J1E7) from the default operating position (covering pins 1 and 2) to the reset/clear position (covering pins 2 and 3).
4. Wait 5 seconds.
5. Remove AC power.
6. Move the jumper back to the default position (covering pins 1 and 2).
7. Close the server chassis.
8. Power up the server.

The BIOS defaults are now restored and can be reset by going into the BIOS setup.

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

7.1.2 Clearing the Password

To clear the password, perform the following steps:

1. Power down the server. Do not unplug the power cord.
2. Open the chassis. For instructions, see your server chassis documentation.
3. Move jumper (J1E8) 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 wait 10 seconds or until POST completes.
6. Power down the server.
7. Open the chassis and move the jumper back to the default position (covering pins 1 and 2).
8. Close the server chassis.
9. Power up the server.

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

7.2 Integrated BMC Force Update Procedure

When performing the standard Integrated BMC firmware update procedure, the update utility places the Integrated BMC into an update mode, allowing the firmware to load safely onto the flash device. In the unlikely event that the Integrated BMC firmware update process fails due to the Integrated BMC not being in the proper update state, the server board provides a BMC Force Update jumper (J1H2), which forces the Integrated BMC into the proper update state. The following procedure should be followed in the event the standard Integrated BMC firmware update process fails or if the Integrated BMC becomes corrupted in such a way as to prevent the system from booting.

1. Power down and remove the AC power cord.
2. Open the server chassis. For instructions, see your server chassis documentation.
3. Move jumper from the default operating position (covering pins 1 and 2) to the enabled position (covering pins 2 and 3).
4. Close the server chassis.
5. Reconnect the AC cord and power up the server.

6. Perform the Integrated BMC firmware update procedure as documented in the README.TXT file that is included in the given Integrated BMC firmware update package. After successful completion of the firmware update process, the firmware update utility may generate an error stating that the Integrated BMC is still in update mode.
7. Power down and remove the AC power cord.
8. Open the server chassis.
9. Move jumper from the enabled position (covering pins 2 and 3) to the disabled position (covering pins 1 and 2).
10. Close the server chassis.
11. Reconnect the AC cord and power up the server.

Note: Normal Integrated BMC functionality is disabled with the Force Integrated BMC Update jumper set to the enabled position. The server should never be run with the BMC Force Update jumper set in this position. This jumper setting should only be used when the standard firmware update process fails. This jumper should remain in the default/disabled position when the server is running normally.

7.3 BIOS Recovery Jumper

In the unlikely event that the BIOS update process fails or the BIOS becomes corrupted and no longer allows the system to POST, the server board provides a BIOS recovery jumper (J1D4), which forces the system to boot from an EFI image provided on a removable media. The following procedure should be followed only in the event the standard BIOS update process fails, the system can no longer boot, and all other recovery methods have been exhausted.

A BIOS recovery can be performed using either a USB Mass Storage device or an El-Torito formatted CD image. Recovery from an USB floppy is not supported.

The following files must be located in the root directory of the recovery media:

- FVMAIN.FV (provided with the BIOS package)
- iFlash32.efi (provided with the BIOS package)
- *Rec.cap (provided with the BIOS package)
- Startup.nsh

  The BIOS##.nsh file provided with the BIOS package must be manually edited in any text editor to point to the *Rec.cap file and renamed to Startup.nsh.

Use the following steps to perform the BIOS recovery:

1. Power OFF the system and remove AC power.
2. Insert the recovery media.
3. Switch the Recovery Jumper (J1D4) to pins 2-3.
4. Reapply AC power and power on the system.

The BIOS POST screen appears displaying progress and the system automatically boots to the EFI shell. The Startup.nsh file executes, updating the BIOS.

5. Once successfully updated, power down the system and remove AC power.
6. Replace the BIOS Recovery Jumper (J1D4) to its default location on pins 1-2.
7. Reapply AC power and power on the system. *DO NOT* interrupt the BIOS POST during the first boot.
8. After a successful boot, reboot the system and press F2 when prompted to enter the BIOS setup and configure any settings.

8. Intel® Light-Guided Diagnostics

The server board has several on-board diagnostic LEDs to assist in troubleshooting board-level issues. This section shows where each LED is located on the server board and describes the function of each LED.

8.1 5-Volt Standby LED

Several server management features of this server board require that a 5-V standby voltage be supplied from the power supply. Some of the features and components that require this voltage be present when the system is "Off" include the Integrated BMC, on-board NICs, and an optional RMM3 connector when Intel® RMM3 is installed.

The LED is located in the lower-left corner of the server board and is labeled "5VSB_LED". It is illuminated when AC power is applied to the platform and 5 volt standby voltage is supplied to the server board by the power supply.

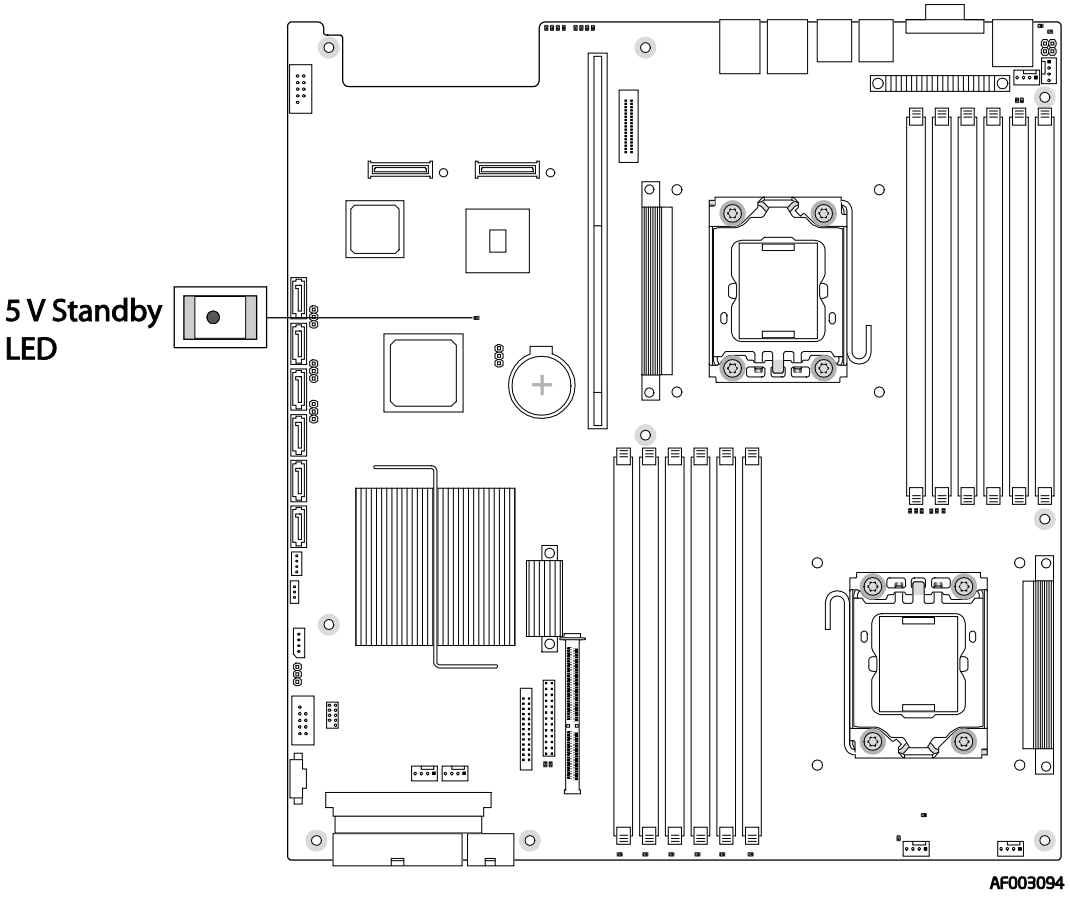


Figure 41. 5-Volt Standby Status LED Location

8.2 Fan Fault LEDs

Fan fault LEDs are present for the six fans and are located near each CPU fan header.

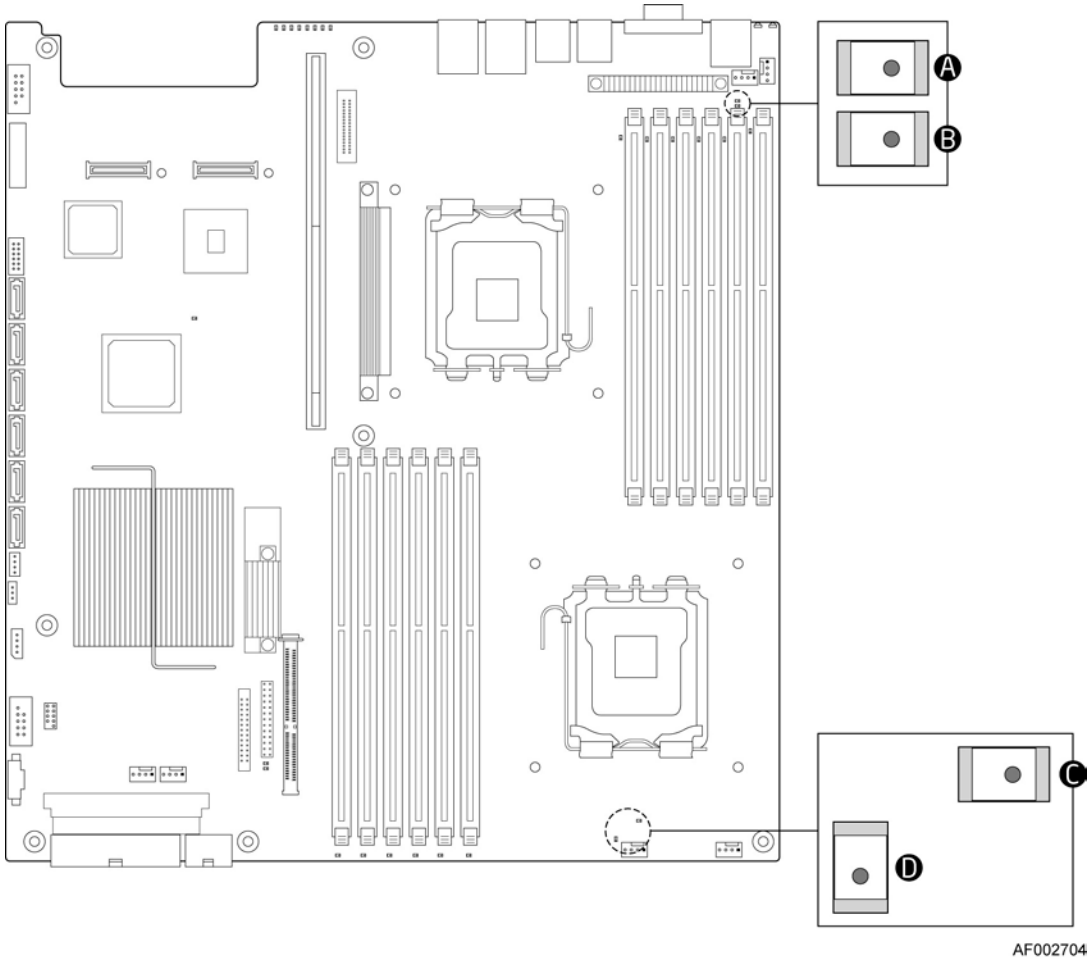


Figure 42. Fan Fault LED Locations

8.3 System Status LED

The server board provides a LED for the system status. The location of the LED is shown in the following figure.

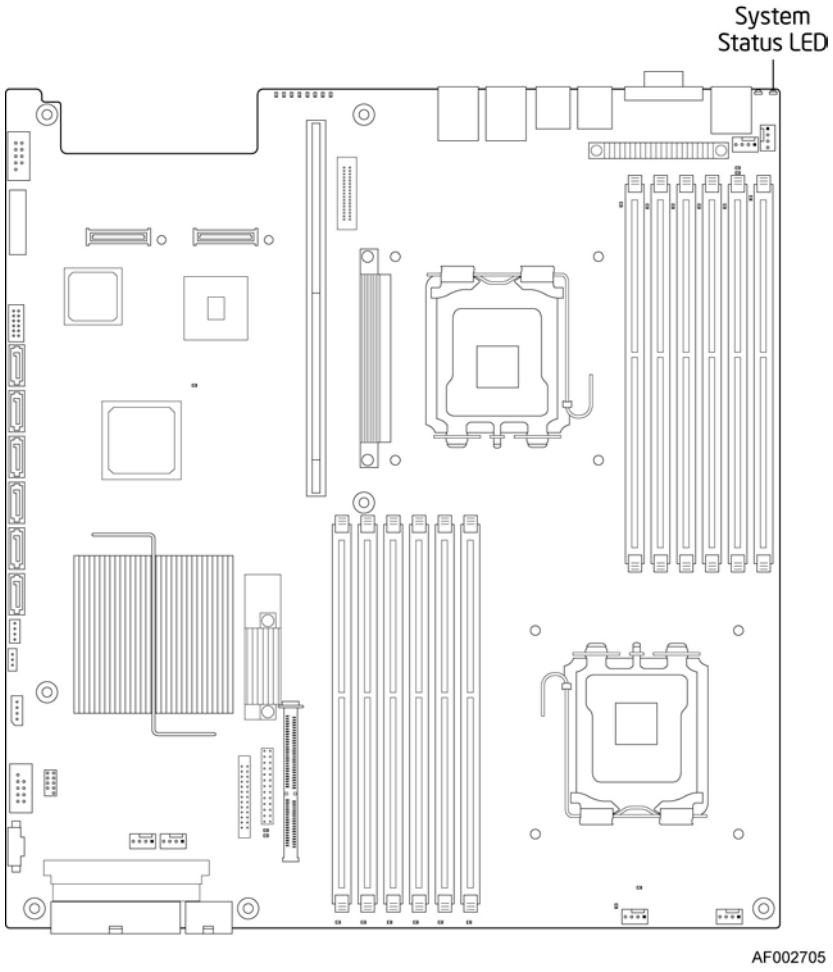


Figure 43. System Status LED Location

The bi-color System Status LED operates as follows:

Table 72. System Status LED

Color	State	Criticality	Description
Off	N/A	Not ready	AC power off.
Green/ Amber	Alternating Blink	Not ready	Pre DC Power On – 20-30 second Integrated BMC Initialization when AC is applied to the server. Control Panel buttons are disabled until Integrated BMC initialization is completed.
Green	Solid on	System OK	System booted and ready.
Green	Blink	Degraded	System degraded ▪ Unable to use all of the installed memory (more than one DIMM installed). ▪ In a mirrored configuration, when memory mirroring takes place and system loses memory redundancy.

Color	State	Criticality	Description
			▪ Redundancy loss such as power supply or fan. This does not apply to non-redundant subsystems. ▪ PCI Express* link errors ▪ CPU failure/disabled – if there are two processors and one of them fails. ▪ Fan alarm – Fan failure. Number of operational fans should be more than the minimum number needed to cool the system. ▪ Non-critical threshold crossed – Temperature and voltage. ▪ Other degraded events (see Appendix B).
Amber	Blink	Non-critical	Non-fatal alarm – system is likely to fail ▪ Critical voltage threshold crossed. ▪ VRD hot asserted. ▪ Minimum numbers of fans to cool the system are not present or have failed. ▪ In a non-mirroring mode, if the threshold of ten correctable errors is crossed within the window. ▪ Other non-critical events (see Appendix B).
Amber	Solid on	Critical, non-recoverable	Fatal alarm – system has failed or shut down ▪ DIMM failure when there is one DIMM present and no good memory is present. ▪ Run-time memory uncorrectable error in non-redundant mode. ▪ IERR signal asserted. ▪ Processor 1 missing ▪ Temperature (e.g., CPU ThermTrip, memory TempHi, critical threshold crossed). ▪ No power good – power fault. ▪ Processor configuration error (for instance, processor stepping mismatch). ▪ Other critical or non-recoverable events (see Appendix B).

8.4 DIMM Fault LEDs

Each DIMM slot has a DIMM Fault LED near the DIMM slot.

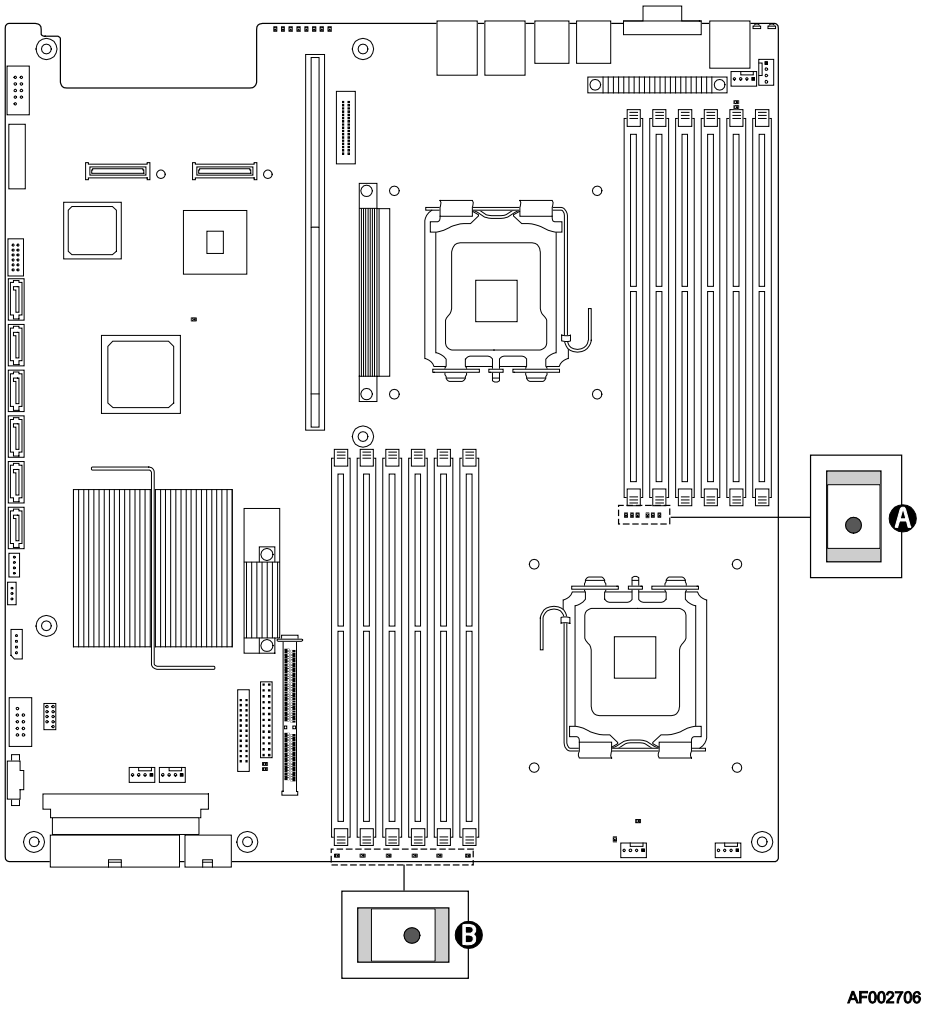
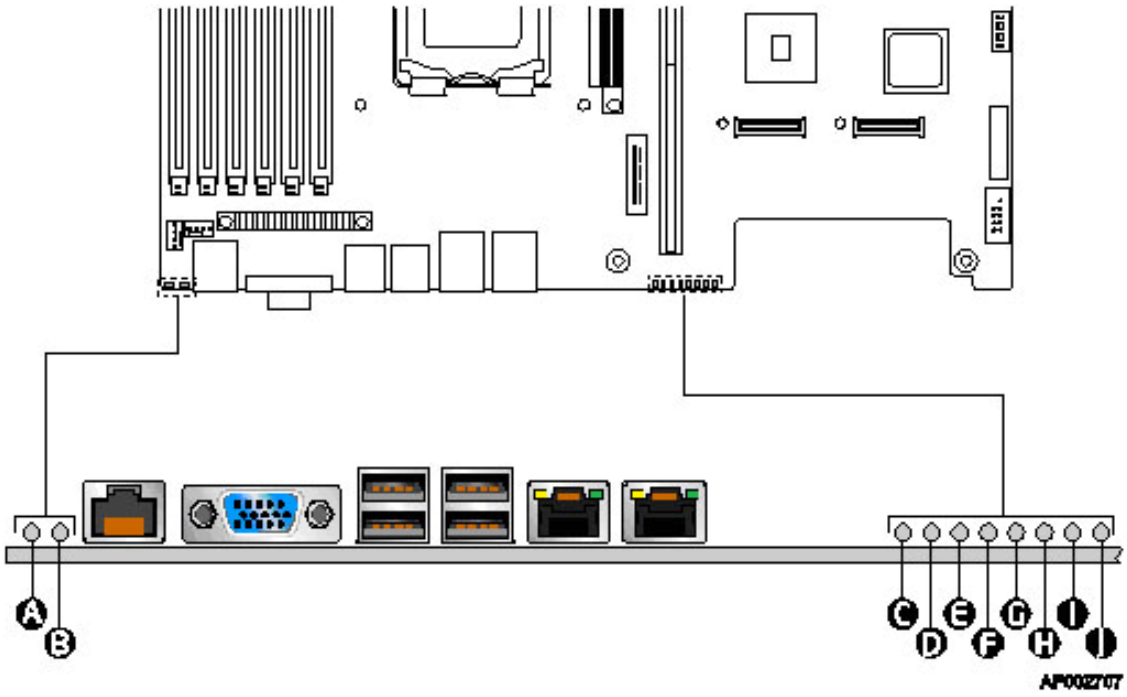


Figure 44. DIMM Fault LED Locations

8.5 Post Code Diagnostic LEDs

Eight amber POST code diagnostic LEDs are located on the back edge of the server board in the rear I/O area of the server board 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 LEDs on the back edge of the server board. To assist in troubleshooting a system hang during the POST process, the diagnostic LEDs can be used to identify the last POST process to be executed. See Appendix C for a complete description of how these LEDs are read, and for a list of all supported POST codes.



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

Figure 45. POST Code Diagnostic LED Location

9. Design and Environmental Specifications

9.1 Intel® Server Board S5520UR, S5520URT Design Specifications

The operation of the server board 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 73. 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: Chassis design must provide proper airflow to avoid exceeding the Intel® Xeon® 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 their published operating or non-operating limits.

9.2 Server Board Power Requirements

This section provides power supply design guidelines for a system using the Intel® Server Board S5520UR, S5520URT, including voltage and current specifications, and power supply on/off sequencing characteristics. The following diagram shows the power distribution implemented on this server board.

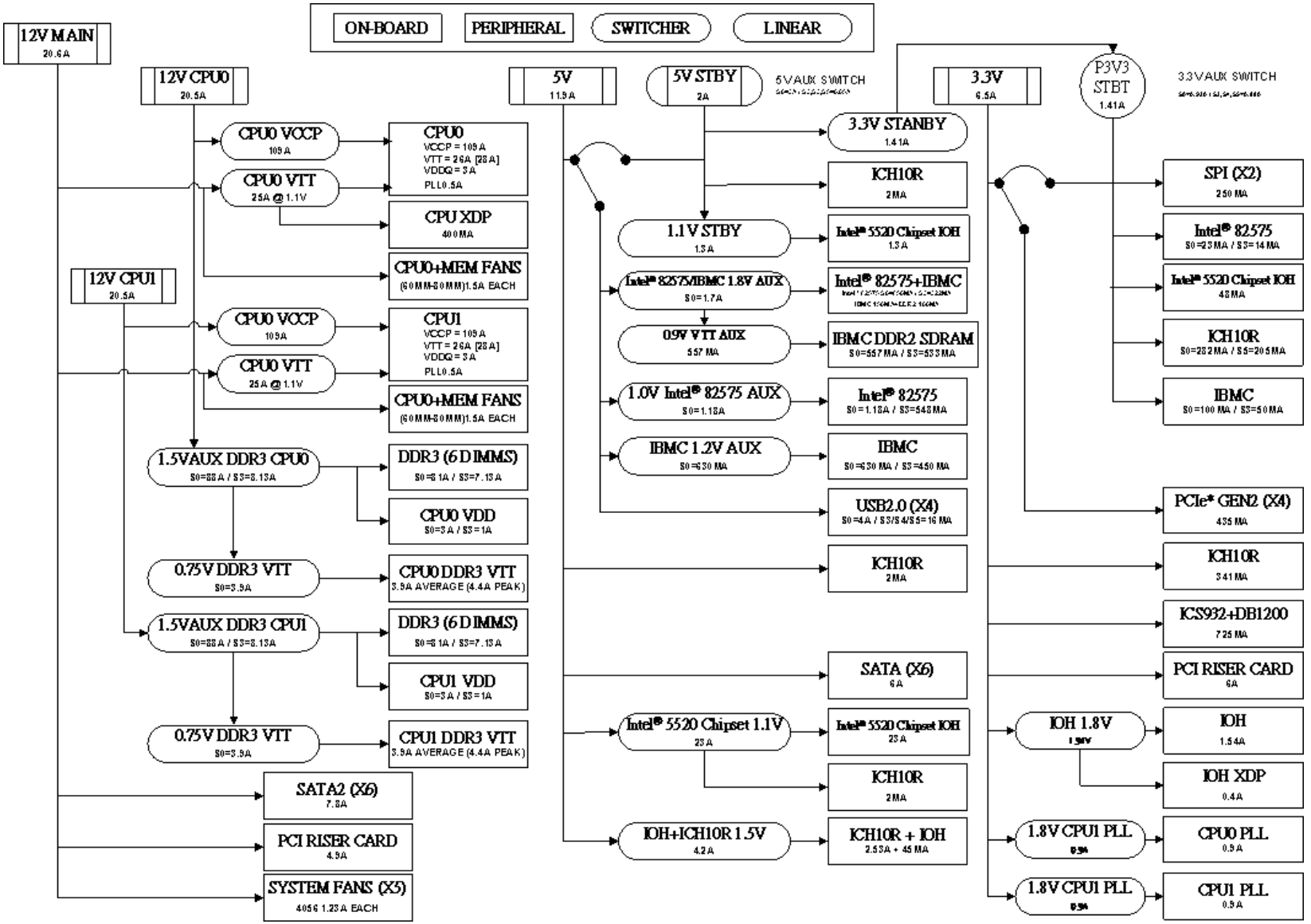


Figure 46. Power Distribution Block Diagram

9.2.1 Processor Power Support

The server board supports the Thermal Design Power (TDP) guideline for Intel® Xeon® processors. The Flexible Motherboard Guidelines (FMB) has also been followed to help determine the suggested thermal and current design values for anticipating future processor needs. The following table provides maximum values for Icc, TDP power, and T_{CASE} for the Intel® Xeon® Processor 5500 Series and Intel® Xeon® Processor 5600 Series.

Table 74. Intel® Xeon® Processor TDP Guidelines

TDP Power	Maximum T_{CASE}	Icc Maximum
130 W	67.0º C	150 A

9.3 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 for use with this server board. This section specifies the power supply requirements Intel® used to develop a power supply for the Intel® Server System SR1600UR.

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

Table 75. 600 W Load Ratings

Voltage	Minimum Continuous	Maximum Continuous	Peak
+3.3 V	1.5 A	20 A	
+5 V	1.0 A	24 A	30 A
+12 V1	0.5 A	24 A	
+12 V2	0.5 A	24 A	
+12 V3	0.5 A	16 A	18 A
+12 V4	0.5 A	16 A	18 A
-12 V	0 A	0.5 A	
+5 VSB	0.1 A	3.0 A	3.5 A

Notes:

1. Maximum continuous total DC output power should not exceed 600 W.
2. Peak load on the combined 12 V output should not exceed 49 A.
3. Maximum continuous load on the combined 12 V output should not exceed 44 A.
4. Peak total DC output power should not exceed 650 W.
5. Peak power and current loading are supported for a minimum of 12 seconds.
6. Combined 3.3 V and 5 V power should not exceed 150 W.

9.3.1 Grounding

The grounds of the power supply output connector pins provide the power return path. The output connector ground pins are connected to safety ground (power supply enclosure). This grounding is designed to ensure passing the maximum allowed common mode noise levels.

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

9.3.2 Standby Outputs

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

9.3.3 Remote Sense

The power supply has remote sense return 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 uses remote sense (3.3 VS) to regulate out drops in the system for the +3.3 V output.

The +5 V, +12 V1, +12 V2, +12 V3, +12V4, –12 V and 5 VSB outputs only use remote sense referenced to the remote sense return 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 a 200 mV drop on the +3.3 V output. The remote sense return must be able to regulate out a minimum of a 200 mV drop in the power ground return. The current in any remote sense line is 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.

9.3.4 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.

Table 76. Voltage Regulation Limits

Parameter	Tolerance	Minimum	Normal	Maximum	Units
+ 3.3V	- 5%/+5%	+3.14	+3.30	+3.46	V_{rms}
+ 5V	- 5%/+5%	+4.75	+5.00	+5.25	V_{rms}
+ 12V1,2,3,4	- 5%/+5%	+11.40	+12.00	+12.60	V_{rms}
- 12V	- 10%/+10%	-10.80	-12.00	-13.20	V_{rms}
+ 5VSB	- 5%/+5%	+4.75	+5.00	+5.25	V_{rms}

9.3.5 Dynamic Loading

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

Table 77. Transient Load Requirements

Output	Step Load Size (See note 2)	Load Slew Rate	Test capacitive Load
+3.3 V	5.0 A	0.25 A/μsec	250 μF
+5 V	6.0 A	0.25 A/μsec	400 μF
12 V1 + 12 V2 + 12 V3 + 12 V4	28.0 A	0.25 A/μsec	2200 μF [1,2]
+5 VSB	0.5 A	0.25 A/μsec	20 μF

Notes:

1. Step loads on each 12 V output may happen simultaneously.
2. The +12 V should be tested with 2200 μF evenly split between the four +12 V rails.

9.3.6 Capacitive Loading

The power supply is stable and meets all requirements with the following capacitive loading ranges.

Table 78. Capacitve Loading Conditions

Output	Minimum	Maximum	Units
+3.3 V	100	6,800	μF
+5 V	10	4,700	μF
+12 V1,2,3,4	220 each	11,000	μF
-12 V	1	350	μF
+5 VSB	20	2000	μF

9.3.7 Closed-loop Stability

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

9.3.8 Common Mode Noise

The Common Mode noise on any output does not exceed 350 mV pk-pk over the frequency band of 10 Hz to 30 MHz.

- The measurement is made across a 100Ω resistor between each of the DC outputs, including ground, at the DC power connector and chassis ground (power subsystem enclosure).
- The test setup uses a FET probe such as Tektronix* model P6046 or equivalent.

9.3.9 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 is placed in parallel to the 0.1 μF ceramic capacitor at the point of measurement.

Table 79. Ripple and Noise

+3.3 V	+5 V	+12 V1,2,3,4	-12 V	+5 VSB
50 mVp-p	50 mVp-p	120 mVp-p	120 mVp-p	50 mVp-p

9.3.10 Timing Requirements

The timing requirements for the power supply operation are as follows:

- The output voltages must rise from 10% to within regulation limits (T_{vout_rise}) within 5 ms to 70 ms, except for 5 VSB, in which case it is allowed to rise from 1.0 ms to 25 ms.
- The +3.3 V, +5 V and +12 V output voltages should start to rise approximately at the same time.
- All outputs must rise monotonically.
- The +5 V output needs to be greater than the +3.3 V output during any point of the voltage rise.
- The +5 V output must never be greater than the +3.3 V output by more than 2.25 V.
- Each output voltage should reach regulation within 50 ms (T_{vout_on}) of each other when the power supply is turned on.
- Each output voltage should fall out of regulation within 400 msec (T_{vout_off}) of each other when the power supply is turned off.and shows 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 80. Output Voltage Timing

Item	Description	Minimum	Maximum	Units
T_{vout_rise}	Output voltage rise time from each main output.	5.0[1]	70[1]	Msec
T_{vout_on}	All main outputs must be within regulation of each other within this time.		50	Msec
T_{vout_off}	All main outputs must leave regulation within this time.		700	Msec

Note:
The 5 VSB output voltage rise time should be from 1.0 ms to 25.0 ms

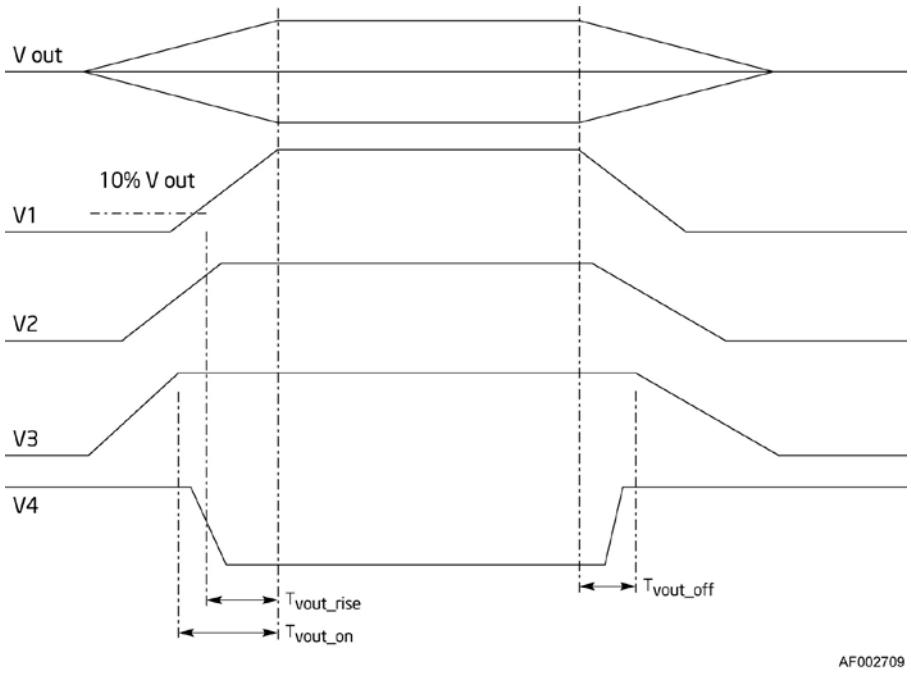


Figure 47. Output Voltage Timing

Table 81. Turn On/Off Timing

Item	Description	Minimum	Maximum	Units
$T_{sb\_on\_delay}$	Delay from AC being applied to 5 VSB being within regulation.		1500	Msec
$T_{ac\_on\_delay}$	Delay from AC being applied to all output voltages being within regulation.		2500	Msec
T_{vout_holdup}	Duration for which all output voltages stay within regulation after loss of AC. Measured at 80% of maximum load.	21		Msec
T_{pwok_holdup}	Delay from loss of AC to de-assertion of PWOK. Measured at 80% of maximum load.	20		Msec
$T_{pson\_on\_delay}$	Delay from PSON# active to output voltages within regulation limits.	5	400	Msec
T_{pson_pwok}	Delay from PSON# deactive to PWOK being de-		50	Msec

Item	Description	Minimum	Maximum	Units
	asserted.			
T_{pwok_on}	Delay from output voltages within regulation limits to PWOK asserted at turn on.	100	500	Msec
T_{pwok_off}	Delay from PWOK de-asserted to output voltages (3.3 V, 5 V, 12 V, -12 V) dropping out of regulation limits.	1		Msec
T_{pwok_low}	Duration of PWOK being in the de-asserted state during an off/on cycle using AC or the PSON signal.	100		Msec
T_{sb_vout}	Delay from 5 VSB being in regulation to O/Ps being in regulation at AC turn on.	50	1000	Msec
T_{5VSB_holdup}	Duration for which the 5 VSB output voltage stays within regulation after loss of AC.	70		Msec

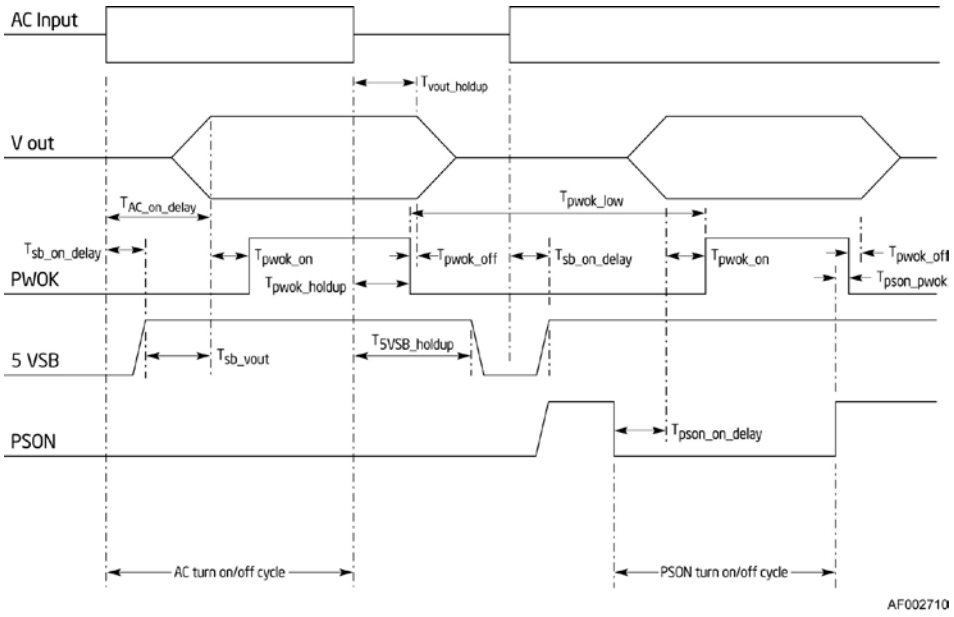


Figure 48. Turn On/Off Timing (Power Supply Signals)

9.3.11 Residual Voltage Immunity in Standby Mode

The power supply is immune to any residual voltage placed on its outputs (typically, a leakage voltage through the system from standby output) up to 500 mV. There is no additional heat generated, nor stressing of any internal components with this voltage applied to any individual output, and all outputs simultaneously. It also does not trip the power supply protection circuits during turn on.

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

9.3.12 Protection Circuits

Protection circuits inside the power supply cause only the power supply's main outputs to shut down. If the power supply latches off due to a protection circuit tripping, an AC cycle OFF for 15 seconds and a PSON# cycle HIGH for 1 second is able to reset the power supply.

9.3.12.1 Over-current Protection (OCP)

The power supply has current limits to prevent the +3.3 V, +5 V, and +12 V outputs from exceeding the values shown in the following table. If the current limits are exceeded, the power supply shuts down and latches off. The latch is cleared by toggling the PSON# signal or by an AC power interruption. The power supply is not damaged from repeated power cycling in this condition. -12 V and 5 VSB are protected under over-current or shorted conditions so that no damage can occur to the power supply. Auto-recovery feature is a requirement on 5 VSB rail.

Table 82. Over-current Protection (OCP)

Voltage	Over-current Limit (I_{out} limit)
+3.3 V	110% minimum (= 22 A) ; 150% maximum (= 30 A)
+5 V	110% min (= 26.4 A); 150% max (= 36 A)
+12 V1	26 A min;
+12 V2	26 A min; 36 A max
+12 V3	18 A min; 20 A max
+12 V4	18 A min; 20 A max
-12 V	0.7 A min; 2.0 A max
5 VSB	115% of rating minimum; 6 A maximum

9.3.12.2 Over-voltage Protection (OVP)

The power supply over-voltage protection is locally sensed. The power supply shuts down and latches off after an over-voltage condition occurs. This latch is cleared by toggling the PSON# signal or by an AC power interruption. The table below contains the over-voltage limits. The values are measured at the output of the power supply's connectors. The voltage never exceeds the maximum levels when measured at the power pins of the power supply connector during any single point of fail. The voltage never trips any lower than the minimum levels when measured at the power pins of the power supply connector.

Exception: +5 VSB rail should be able to recover after an over-voltage condition occurs.

Table 83. Over-voltage Protection (OVP) Limits

Output Voltage	Minimum (V)	Maximum (V)
+3.3 V	3.9	4.5
+5 V	5.7	6.2
+12 V1,2, 3, 4	13.3	14.5
-12 V	-13.3	-14.5
+5 VSB	5.7	6.5

10. Regulatory and Certification Information

10.1 Product Regulation Requirements

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

10.1.1 Product Safety Compliance

The Intel® Server Board S5520UR, S5520URT complies 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)
- GOST R 50377-92 – Listed on one System Certification (Russia)
- Belarus Certification – Listed on System Certification (Belarus)
- CE - Low Voltage Directive 73/23/EEE (Europe)
- IRAM Certification (Argentina)

10.1.2 Product EMC Compliance – Class A Compliance

- 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)
- GOST R 29216-91 Emissions - Listed on one System Certification (Russia)
- GOST R 50628-95 Immunity –Listed on one System Certification (Russia)
- Belarus Certification – Listed on one System Certification (Belarus)
- KCC (EMI) (Korea)

10.1.3 Certifications/Registrations/Declarations

- NRTL Certification (US/Canada)
- 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)
- GOST – Listed on one System Certification (Russia)
- Belarus – Listed on one System Certification (Belarus)
- KCC Certification (Korea)
- Ecology Declaration (International)

10.2 Product Regulatory Compliance Markings

This Intel® Server Board bears the following regulatory marks:

Regulatory Compliance	Country	Marking
UL Mark	USA/Canada	
CE Mark	Europe	
FCC Marking (Class A)	USA	This device complies with Part 15 of the FCC Rules. Operation of this device 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. Manufactured by Intel Corporation
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
KCC Mark	Korea	

10.3 Electromagnetic Compatibility Notices

10.3.1 FCC Verification Statement (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

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 into an outlet on a circuit different from that 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.

10.3.2 ICES-003 (Canada)

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe Aprescrites dans la norme sur le matériel brouilleur:

"Appareils Numériques", NMB-003 édictée 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.

10.3.3 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.

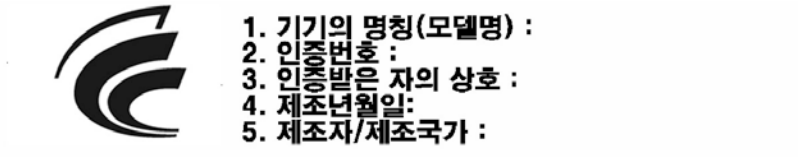
10.3.4 BSMI (Taiwan)

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

10.3.5 KCC (Korea)

Following is the KCC certification information for Korea.



English translation of the notice above:

1. Type of Equipment (Model Name): On Certification and Product
2. Certification No.: On KCC certificate. Obtain certificate from local Intel representative
3. Name of Certification Recipient: Intel Corporation
4. Date of Manufacturer: Refer to date code on product
5. Manufacturer/Nation: Intel Corporation/Refer to country of origin marked on product

Appendix A: Integration and Usage Tips

- When adding or removing components or peripherals from the server board, AC power must be removed. With AC power plugged into the server board, 5-V standby is still present even though the server board is powered off.
- This server board only supports The Intel® Xeon® Processor 5500 Series and Intel® Xeon® Processor 5600 Series with 130 W and less Thermal Design Power (TDP). Previous generations of the Intel® Xeon® processors are not supported.
- Processors must be installed in order. CPU 1 is located near the rear of the server board and must be populated to operate the board.
- On the back edge of the server board are eight diagnostic LEDs that display a sequence of amber POST codes during the boot process. If the server board hangs during POST, the LEDs displays the last POST event run before the hang.
- This server board only supports registered DDR3 DIMMs (RDIMMs) and unbuffered DDR3 DIMMs (UDIMMs). Mixing of RDIMMs and UDIMMs is not supported.
- For the best performance, the number of DDR3 DIMMs installed should be balanced across both processor sockets and memory channels. For example, a two-DIMM configuration performs better than a one-DIMM configuration. In a two-DIMM configuration, DIMMs should be installed in DIMM sockets A1 and D1. A six-DIMM configuration (DIMM sockets A1, B1, C1, D1, E1, and F1) performs better than a three-DIMM configuration (DIMM sockets A1, B1, and C1).
- The Intel® Remote Management Module 3 (Intel® RMM3) connector is not compatible with the Intel® Remote Management Module (Product Order Code - AXXRMM) or Intel® Remote Management Module 2 (Product Order Code - AXXRMM2).
- Clear the CMOS with AC power cord plugged. Removing the AC power before performing the CMOS clear operation causes the system to automatically power up and immediately power down after the CMOS clear procedure is followed and AC power is re-applied. If this happens, remove the AC power cord, wait 30 seconds, and then re-connect the AC power cord. Power up the system and proceed to the <F2> BIOS Setup utility to reset the desired settings.
- Normal Integrated BMC functionality is disabled with the BMC Force Update jumper (J1H1) set to the “enabled” position (pins 2-3). The server should never be run with the BMC Force Update jumper set in this position and should only be used when the standard firmware update process fails. This jumper should remain in the default (disabled) position (pins 1-2) when the server is running normally.
- This server board no longer supports the rolling BIOS (two BIOS banks) and implements a BIOS recovery mechanism instead.
- When performing a normal BIOS update procedure, the BIOS recovery jumper (J1E5) must be set to its default position (pins 1-2).

Appendix B: Integrated 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 values are the values enumerated in the *Sensor Type Codes* table in the IPMI specification. The Sensor Type provides the context in which to interpret the sensor, such as the physical entity or characteristic that is represented by this sensor.

- **Event/Reading Type**

  The Event/Reading Type values are from the *Event/Reading Type Code Ranges* and *Generic Event/Reading Type Codes* tables in the IPMI specification. Digital sensors are a specific type of discrete sensor, which have only two states.

- **Event Offset/Triggers**

  Event Thresholds are event-generating thresholds for threshold types of sensors.

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

  Event Triggers are supported event-generating offsets for discrete type sensors. The offsets can be found in the *Generic Event/Reading Type Codes* or *Sensor Type Codes* tables in the IPMI specification, 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 Value indicates the type of value returned for threshold and other non-discrete type sensors.
  - Readable Offsets indicate the offsets for discrete sensors that are readable 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 that is 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 for a sensor to be rechecked and updated upon a transition between good and bad states. Rearming the sensors can be done manually or automatically. This column indicates the type supported by the sensor. The following abbreviations are used to describe a sensor:

  - A: Auto-rearm
  - M: Manual rearm

- **Default Hysteresis**

  The hysteresis setting applies to all thresholds of the sensor. This column provides the count of hysteresis for the sensor, which can be 1 or 2 (positive or negative hysteresis).

- **Criticality**

  Criticality is a classification of the severity and nature of the condition. It also controls the behavior of the Control Panel Status LED.

- **Standby**

  Some sensors operate on standby power. These sensors may be accessed and/or generate events when the main (system) power is off, but AC power is present.

Table 84. Integrated BMC Core Sensors

Sensor Name	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 Stat	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 Redundancy	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-red: suff res from redud	Degraded					
					04 - Non-red: suff from insuff	Degraded					
					05 - Non-red: insufficient	Fatal					
					06 - Redun degrade from fully redun	Degraded					
					07 – Redun degrade from non-redundant	Degraded					

Sensor Name	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
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 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 least lost	Degraded					
FP Interrupt (NMI)	05h	All	Critical Interrupt 13h	Sensor Specific 6Fh	00 - Front panel NMI/diagnostic interrupt	OK	As	–	Trig Offset	A	–
SMI Timeout	06h	All	SMI Timeout F3h	Digital Discrete 03h	01 – State asserted	Fatal	As and De	–	Trig Offset	A	–
System Event Log	07h	All	Event Logging Disabled 10h	Sensor Specific 6Fh	02 - Log area reset/cleared	OK	As	–	Trig Offset	A	X
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	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	12h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–

Sensor Name	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 +1.5V 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	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	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	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	17h	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
BB Vbat	18h	All	Voltage 02h	Generic 05h	01 - Limit exceeded	Non-fatal	As and De	–	Trig Offset	A	X
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	–
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	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	1Ch	All	Voltage 02h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	–

Sensor Name	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
Server board Temp	20h	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
IOH Temp	21h	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Front Panel Temp	22h	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
MEM P1 THRM MRGN	23h	All	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
MEM P2 THRM MRGN	24h	Dual processor only	Temperature 01h	Threshold 01h	[u,l] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
Fan Tach Sensors	30h–39h	Chassis-specific	Fan 04h	Threshold 01h	[l] [c,nc]	nc = Degraded c = Non-fatal[2]	As and De	Analog	R, T	M	
Fan Present Sensors	40h–45h	Chassis-specific	Fan 04h	Generic 08h	01 - Device inserted	OK	As and De	-	Triggered Offset	Auto	–
Fan Redundancy	46h	Chassis-specific	Fan 04h	Generic 0Bh	00 - Fully redundant	OK	As and De	–	Trig Offset	A	X
					01 - Redundancy lost	Degraded					
					02 - Redundancy degraded	Degraded					
					03 - Non-red: suff res from redund	Degraded					

Sensor Name	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
					04 - Non-red: suff from insuff	Degraded					
					05 - Non-red: Insufficient	Non-fatal					
					06 - Redun degrade from full	Degraded					
					07 – Redun degrade from non-redundant	Degraded					
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					
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					
PS1 Power In	52h	Chassis-specific	Power Supply 08h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
PS2 Power In	53h	Chassis-specific	Power Supply 08h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X

Sensor Name	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
PS1 Current Out	54h	Chassis-specific	Power Supply 08h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
PS2 Current Out	55h	Chassis-specific	Power Supply 08h	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
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
PS2 Temperature	57h	Chassis-specific	Temperature	Threshold 01h	[u] [c,nc]	nc = Degraded c = Non-fatal	As and De	Analog	R, T	A	X
P1 Status	60h	All	Processor 07h	Sensor Specific 6Fh	01 - Thermal trip 07 - Presence	Fatal OK	As and De	–	Trig Offset	M	X
P2 Status	61h	Dual processor only	Processor 07h	Sensor Specific 6Fh	01- Thermal trip 07 - Presence	Fatal OK	As and De	–	Trig Offset	M	X
P1 Therm Margin	62h	All	Temperature 01h	Threshold 01h	–	–	–	Analog	–	–	–
P2 Therm Margin	63h	Dual processor only	Temperature 01h	Threshold 01h	–	–	–	Analog	–	–	–
P1 Therm Ctrl %	64h	All	Temperature 01h	Threshold 01h	[u] [c]	Non-fatal	As and De	Analog	Trig Offset	A	–
P2 Therm Ctrl %	65h	Dual processor only	Temperature 01h	Threshold 01h	[u] [c]	Non-fatal	As and De	Analog	Trig Offset	A	–
P1 VRD Temp	66h	All	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Fatal	As and De	–	Trig Offset	M	–

Sensor Name	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
P2 VRD Temp	67h	Dual processor only	Temperature 01h	Digital Discrete 05h	01 - Limit exceeded	Fatal	As and De	–	Trig Offset	M	–
CATERR	68h	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	Non-fatal	As and De	–	Trig Offset	M	–
CPU Missing	69h	All	Processor 07h	Digital Discrete 03h	01 – State Asserted	Non-fatal	As and De	–	Trig Offset	M	–
IOH Thermal Trip	6Ah	All	Temperature 01h	Digital Discrete 03h	01 – State Asserted	Fatal	As and De	–	Trig Offset	M	–

Appendix C: Management Engine Generated SEL Event Messages

This appendix lists the OEM System Event Log message format of events generated by the Management Engine (ME). This includes the definition of event data bytes 10-16 of the Management Engine generated SEL records. For System Event Log format information, see the *Intelligent Platform Management Interface Specification, Version 2.0*.

Table 85. Server Platform Services Firmware Health Event

Server Platform Services Firmware Health Event	**Request**
	Byte 1 - EvMRev =04h (IPMI2.0 format) Byte 2 – Sensor Type =DCh (OEM) Byte 3 – Sensor Number =23 – Server Platform Services Firmware Health Byte 4 – Event Dir | Event Type [7] – Event Dir =0 Assertion Event [6-0] – Event Type =75h (OEM) Byte 5 – Event Data 1 [7,6]=10b – OEM code in byte 2 [5,4]=10b – OEM code in byte 3 [3..0] – Health Event Type =00h –Firmware Status Byte 6 – Event Data 2 =0 - Forced GPIO recovery. Recovery Image loaded due to MGPIO<n> (default recovery pin is MGPIO1) pin asserted. *Repair action: Deassert MGPIO1 and reset the ME* =1 - Image execution failed. Recovery Image loaded because operational image is corrupted. This may be either caused by Flash device corruption or failed upgrade procedure. *Repair action: Either the Flash device must be replaced (if error is persistent) or the upgrade procedure must be started again.* =2 - Flash erase error. Error during Flash erases procedure probably due to Flash part corruption. *Repair action: The Flash device must be replaced.* =3 – Flash corrupted. Error while checking Flash consistency probably due to Flash part corruption. *Repair action: The Flash device must be replaced (if error is persistent).* =4 – Internal error. Error during firmware execution. *Repair action: FW Watchdog Timeout* *Operational image shall be upgraded to other version or hardware board repair is needed (if error is persistent).*

	=5..255 – Reserved Byte 7 – Event Data 3 =<Extended error code. Should be used when reporting an error to the support>

Table 86. Node Manager Health Event

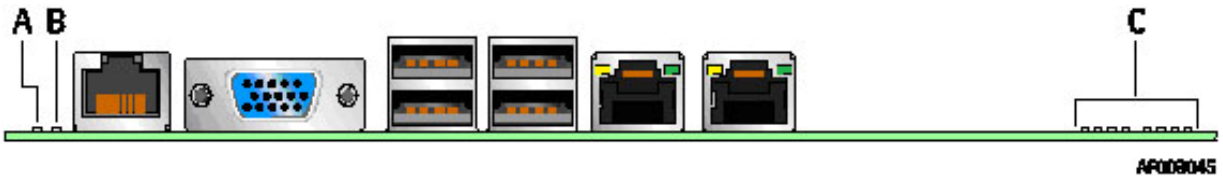
Node Manager Health Event	**Request**
	Byte 1 - EvMRev =04h (IPMI2.0 format) Byte 2 – Sensor Type =DCh (OEM) Byte 3 – Sensor Number (Node Manager Health sensor) Byte 4 – Event Dir | Event Type [0:6] – Event Type = 73h (OEM) [7] – Event Dir =0 Assertion Event Byte 5 – Event Data 1 [0:3] – Health Event Type =02h – Sensor Node Manager [4:5]=10b – OEM code in byte 3 [6:7]=10b – OEM code in byte 2 Byte 6 – Event Data 2 [0:3] – Domain Id (Currently, supports only one domain, Domain 0) [4:7] – Error type =0-9 - Reserved =10 – Policy Misconfiguration =11 – Power Sensor Reading Failure =12 – Inlet Temperature Reading Failure =13 – Host Communication error =14 – Real-time clock synchronization failure =15 – Reserved Byte 7 – Event Data 3 if error indication = 10 <PolicyId> if error indication = 11 <PowerSensorAddress> if error indication = 12 <InletSensorAddress> Otherwise set to 0.

Appendix D: POST Code Diagnostic LED Decoder

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

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

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



A. Status LED
B. ID LED
C. Diagnostic LEDs

Figure 49. Diagnostic LED Placement Diagram

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

Table 87. POST Progress Code LED Example

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

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

Table 88. Diagnostic LED POST Code Decoder

Checkpoint	Diagnostic LED Decoder 0 = On, X=Off								Description
	Upper Nibble				Lower Nibble				
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
Multi-use code (This POST Code is used in different contexts)									
0xF2h	O	O	O	O	X	X	O	X	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)									
0xE8h	O	O	O	X	O	X	X	X	No Usable Memory Error: No memory in the system, or SPD bad so no memory could be detected
0xEAh	O	O	O	X	O	X	O	X	Channel Training Error: DQ/DQS training failed on a channel during memory channel initialization.
0xEBh	O	O	O	X	O	X	O	O	Memory Test Error: memory failed Hardware BIST.
0xEDh	O	O	O	X	O	O	X	O	Population Error: RDIMMs and UDIMMs cannot be mixed in the system
0xEEh	O	O	O	X	O	O	O	X	Mismatch Error: more than 2 Quad Ranked DIMMS in a channel.
Memory Reference Code Progress Codes (Not accompanied by a beep code)									
0xB0h	O	X	O	O	X	X	X	X	Chipset Initialization Phase
0xB1h	O	X	O	O	X	X	X	O	Reset Phase
0xB2h	O	X	O	O	X	X	O	X	DIMM Detection Phase
0xB3h	O	X	O	O	X	X	O	O	Clock Initialization Phase
0xB4h	O	X	O	O	X	O	X	X	SPD Data Collection Phase
0xB6h	O	X	O	O	X	O	O	X	Rank Formation Phase
0xB8h	O	X	O	O	O	X	X	X	Channel Training Phase
0xB9h	O	X	O	O	O	X	X	O	Memory Test Phase
0xBAh	O	X	O	O	O	X	O	X	Memory Map Creation Phase
0xBBh	O	X	O	O	O	X	O	O	RAS Initialization Phase
0xBFh	O	X	O	O	O	O	O	O	MRC Complete
Host Processor									
0x04h	X	X	X	X	X	O	X	X	Early processor initialization where system BSP is selected
0x10h	X	X	X	O	X	X	X	X	Power-on initialization of the host processor (bootstrap processor)
0x11h	X	X	X	O	X	X	X	O	Host processor cache initialization (including AP)
0x12h	X	X	X	O	X	X	O	X	Starting application processor initialization
0x13h	X	X	X	O	X	X	O	O	SMM initialization
Chipset									
0x21h	X	X	O	X	X	X	X	O	Initializing a chipset component
Memory									
0x22h	X	X	O	X	X	X	O	X	Reading configuration data from memory (SPD on DIMM)
0x23h	X	X	O	X	X	X	O	O	Detecting presence of memory
0x24h	X	X	O	X	X	O	X	X	Programming timing parameters in the memory controller
0x25h	X	X	O	X	X	O	X	O	Configuring memory parameters in the memory controller
0x26h	X	X	O	X	X	O	O	X	Optimizing memory controller settings
0x27h	X	X	O	X	X	O	O	O	Initializing memory, such as ECC init

Checkpoint	Diagnostic LED Decoder 0 = On, X=Off								Description
	Upper Nibble				Lower Nibble				
	MSB							LSB	
	8h	4h	2h	1h	8h	4h	2h	1h	
LED	#7	#6	#5	#4	#3	#2	#1	#0	
0x28h	X	X	O	X	O	X	X	X	Testing memory
PCI Bus									
0x50h	X	O	X	O	X	X	X	X	Enumerating PCI busses
0x51h	X	O	X	O	X	X	X	O	Allocating resources to PCI busses
0x52h	X	O	X	O	X	X	O	X	Hot Plug PCI controller initialization
0x53h	X	O	X	O	X	X	O	O	Reserved for PCI bus
0x54h	X	O	X	O	X	O	X	X	Reserved for PCI bus
0x55h	X	O	X	O	X	O	X	O	Reserved for PCI bus
0x56h	X	O	X	O	X	O	O	X	Reserved for PCI bus
0x57h	X	O	X	O	X	O	O	O	Reserved for PCI bus
USB									
0x58h	X	O	X	O	O	X	X	X	Resetting USB bus
0x59h	X	O	X	O	O	X	X	O	Reserved for USB devices
ATA/ATAPI/SATA									
0x5Ah	X	O	X	O	O	X	O	X	Resetting SATA bus and all devices
0x5Bh	X	O	X	O	O	X	O	O	Reserved for ATA
SMBUS									
0x5Ch	X	O	X	O	O	O	X	X	Resetting SMBUS
0x5Dh	X	O	X	O	O	O	X	O	Reserved for SMBUS
Local Console									
0x70h	X	O	O	O	X	X	X	X	Resetting the video controller (VGA)
0x71h	X	O	O	O	X	X	X	O	Disabling the video controller (VGA)
0x72h	X	O	O	O	X	X	O	X	Enabling the video controller (VGA)
Remote Console									
0x78h	X	O	O	O	O	X	X	X	Resetting the console controller
0x79h	X	O	O	O	O	X	X	O	Disabling the console controller
0x7Ah	X	O	O	O	O	X	O	X	Enabling the console controller
Keyboard (only USB)									
0x90h	O	X	X	O	X	X	X	X	Resetting the keyboard
0x91h	O	X	X	O	X	X	X	O	Disabling the keyboard
0x92h	O	X	X	O	X	X	O	X	Detecting the presence of the keyboard
0x93h	O	X	X	O	X	X	O	O	Enabling the keyboard
0x94h	O	X	X	O	X	O	X	X	Clearing keyboard input buffer
0x95h	O	X	X	O	X	O	X	O	Instructing keyboard controller to run Self Test (PS2 only)
Mouse (only USB)									
0x98h	O	X	X	O	O	X	X	X	Resetting the mouse
0x99h	O	X	X	O	O	X	X	O	Detecting the mouse
0x9Ah	O	X	X	O	O	X	O	X	Detecting the presence of mouse
0x9Bh	O	X	X	O	O	X	O	O	Enabling the mouse
Fixed Media									
0xB0h	O	X	O	O	X	X	X	X	Resetting fixed media device
0xB1h	O	X	O	O	X	X	X	O	Disabling fixed media device
0xB2h	O	X	O	O	X	X	O	X	Detecting presence of a fixed media device (hard drive detection, etc.)

Checkpoint	Diagnostic LED Decoder O = On, X=Off Upper Nibble MSB 8h				Lower Nibble 8h			LSB 1h	Description
LED	#7	#6	#5	#4	#3	#2	#1	#0	
0xB3h	O	X	O	O	X	X	O	O	Enabling/configuring a fixed media device
Removable Media									
0xB8h	O	X	O	O	O	X	X	X	Resetting removable media device
0xB9h	O	X	O	O	O	X	X	O	Disabling removable media device
0xBAh	O	X	O	O	O	X	O	X	Detecting presence of a removable media device (CDROM detection, etc.)
0xBCh	O	X	O	O	O	O	X	X	Enabling/configuring a removable media device
Boot Device Selection (BDS)									
0xD0	O	O	X	O	X	X	X	X	Trying to boot device selection 0
0xD1	O	O	X	O	X	X	X	O	Trying to boot device selection 1
0xD2	O	O	X	O	X	X	O	X	Trying to boot device selection 2
0xD3	O	O	X	O	X	X	O	O	Trying to boot device selection 3
0xD4	O	O	X	O	X	O	X	X	Trying to boot device selection 4
0xD5	O	O	X	O	X	O	X	O	Trying to boot device selection 5
0xD6	O	O	X	O	X	O	O	X	Trying to boot device selection 6
0xD7	O	O	X	O	X	O	O	O	Trying to boot device selection 7
0xD8	O	O	X	O	O	X	X	X	Trying to boot device selection 8
0xD9	O	O	X	O	O	X	X	O	Trying to boot device selection 9
0xDA	O	O	X	O	O	X	O	X	Trying to boot device selection A
0xDB	O	O	X	O	O	X	O	O	Trying to boot device selection B
0xDC	O	O	X	O	O	O	X	X	Trying to boot device selection C
0xDD	O	O	X	O	O	O	X	O	Trying to boot device selection D
0xDE	O	O	X	O	O	O	O	X	Trying to boot device selection E
0xDF	O	O	X	O	O	O	O	O	Trying to boot device selection F
Pre-EFI Initialization (PEI) Core									
0xE0h	O	O	O	X	X	X	X	X	Started dispatching early initialization modules (PEIM)
0xE1h	O	O	O	X	X	X	X	O	Reserved for initialization module use (PEIM)
0xE2h	O	O	O	X	X	X	O	X	Initial memory found, configured, and installed correctly
0xE3h	O	O	O	X	X	X	O	O	Reserved for initialization module use (PEIM)
Driver eXecution Environment (DXE) Core (not accompanied by a beep code)									
0xE4h	O	O	O	X	X	O	X	X	Entered EFI driver execution phase (DXE)
0xE5h	O	O	O	X	X	O	X	O	Started dispatching drivers
0xE6h	O	O	O	X	X	O	O	X	Started connecting drivers
DXE Drivers									
0xE7h	O	O	O	X	O	O	X	O	Waiting for user input
0xE8h	O	O	O	X	O	X	X	X	Checking password
0xE9h	O	O	O	X	O	X	X	O	Entering BIOS setup
0xEAh	O	O	O	X	O	X	O	X	Flash Update
0xEEh	O	O	O	X	O	O	O	X	Calling Int 19. One beep unless silent boot is enabled.
0xEFh	O	O	O	X	O	O	O	O	Unrecoverable boot failure
Runtime Phase/EFI Operating System Boot									
0xF2h	O	O	O	O	X	X	O	X	Signal that the OS has switched to virtual memory mode
0xF4h	O	O	O	O	X	O	X	X	Entering Sleep state

Checkpoint	Diagnostic LED Decoder O = On, X=Off Upper Nibble MSB 8h	4h	2h	1h	Lower Nibble 8h	4h	2h	LSB 1h	Description
LED	#7	#6	#5	#4	#3	#2	#1	#0	
0xF5h	O	O	O	O	X	O	X	O	Exiting Sleep state
0xF8h	O	O	O	O	O	X	X	X	OS has requested EFI to close boot services (ExitBootServices ( ) Has been called)
0xF9h	O	O	O	O	O	X	X	O	OS has switched to virtual address mode (SetVirtualAddressMap ( ) Has been called)
0xFAh	O	O	O	O	O	X	O	X	OS has requested the system to reset (ResetSystem ( ) has been called)
Pre-EFI Initialization Module (PEIM)/Recovery									
0x30h	X	X	O	O	X	X	X	X	Crisis recovery has been initiated because of a user request
0x31h	X	X	O	O	X	X	X	O	Crisis recovery has been initiated by software (corrupt flash)
0x34h	X	X	O	O	X	O	X	X	Loading crisis recovery capsule
0x35h	X	X	O	O	X	O	X	O	Handing off control to the crisis recovery capsule
0x3Fh	X	X	O	O	O	O	O	O	Unable to complete crisis recovery capsule

Appendix E: POST Code Errors

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 that is being initialized. The operation field represents the specific initialization activity. Based on the data bit availability to display progress codes, a progress code can be customized 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 progress codes may be reported by the system BIOS or option ROMs.

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

- **No Pause:** The message is displayed on the screen during POST or on the Error Manager screen. The system continues booting with a degraded state. The user may want to replace the erroneous unit. The setup POST error Pause setting does not have any effect with this error.
- **Pause:** The message is displayed on the Error Manager screen, and an error is logged to the SEL. The setup POST error Pause setting determines whether the system pauses to the Error Manager for this type of error, where the user can take immediate corrective action or choose to continue booting.
- **Halt:** The message is displayed on the Error Manager screen, an error is logged to the SEL, and the system cannot boot unless the error is resolved. The user needs to replace the faulty part and restart the system. The setup POST error Pause setting does not have any effect with this error.

Table 89. POST Error Messages and Handling

Error Code	Error Message	Response
0012	CMOS date/time not set	Pause
0048	Password check failed	Halt
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 cannot 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	L3 cache size mismatch	Halt
0194	CPUID, processor family are different	Halt
0195	Front side bus mismatch	Pause
0196	Processor Model mismatch	Pause
0197	Processor speeds mismatched	Pause
0198	Processor family is unsupported.	Pause
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
8110	Processor 01 internal error (IERR) on last boot	Pause
8111	Processor 02 internal error (IERR) on last boot	Pause
8120	Processor 01 thermal trip error on last boot	Pause
8121	Processor 02 thermal trip error on last boot	Pause
8130	Processor 01 disabled	Pause
8131	Processor 02 disabled	Pause

Error Code	Error Message	Response
8140	Processor 01 Failed FRB-3 Timer.	No Pause
8141	Processor 02 Failed FRB-3 Timer.	No Pause
8160	Processor 01 unable to apply BIOS update	Pause
8161	Processor 02 unable to apply BIOS update	Pause
8170	Processor 01 failed Self Test (BIST).	Pause
8171	Processor 02 failed Self Test (BIST).	Pause
8180	Processor 01 BIOS does not support the current stepping for processor	No Pause
8181	Processor 02 BIOS does not support the current stepping for processor	No Pause
8190	Watchdog timer failed on last boot	Pause
8198	Operating system boot watchdog timer expired on last boot	Pause
8300	Integrated Baseboard Management Controller failed self-test	Pause
84F2	Integrated Baseboard Management Controller failed to respond	Pause
84F3	Integrated 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_A3 failed Self Test (BIST).	Pause
8523	DIMM_A4 failed Self Test (BIST).	Pause
8524	DIMM_B1 failed Self Test (BIST).	Pause
8525	DIMM_B2 failed Self Test (BIST).	Pause
8526	DIMM_B3 failed Self Test (BIST).	Pause
8527	DIMM_B4 failed Self Test (BIST).	Pause
8528	DIMM_C1 failed Self Test (BIST).	Pause
8529	DIMM_C2 failed Self Test (BIST).	Pause
852A	DIMM_C3 failed Self Test (BIST).	Pause
852B	DIMM_C4 failed Self Test (BIST).	Pause
852C	DIMM_D1 failed Self Test (BIST).	Pause
852D	DIMM_D2 failed Self Test (BIST).	Pause
852E	DIMM_D3 failed Self Test (BIST).	Pause
852F	DIMM_D4 failed Self Test (BIST).	Pause
8540	DIMM_A1 Disabled.	Pause
8541	DIMM_A2 Disabled.	Pause
8542	DIMM_A3 Disabled.	Pause
8543	DIMM_A4 Disabled.	Pause
8544	DIMM_B1 Disabled.	Pause
8545	DIMM_B2 Disabled.	Pause
8546	DIMM_B3 Disabled.	Pause
8547	DIMM_B4 Disabled.	Pause
8548	DIMM_C1 Disabled.	Pause
8549	DIMM_C2 Disabled.	Pause
854A	DIMM_C3 Disabled.	Pause
854B	DIMM_C4 Disabled.	Pause
854C	DIMM_D1 Disabled.	Pause
854D	DIMM_D2 Disabled.	Pause
854E	DIMM_D3 Disabled.	Pause
854F	DIMM_D4 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_A3 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8563	DIMM_A4 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8564	DIMM_B1 Component encountered a Serial Presence Detection (SPD) fail error.	Pause

Error Code	Error Message	Response
8565	DIMM_B2 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8566	DIMM_B3 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8567	DIMM_B4 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8568	DIMM_C1 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8569	DIMM_C2 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
856A	DIMM_C3 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
856B	DIMM_C4 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
856C	DIMM_D1 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
856D	DIMM_D2 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
856E	DIMM_D3 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
856F	DIMM_D4 Component encountered a Serial Presence Detection (SPD) fail error.	Pause
8580	DIMM_A1 Correctable ECC error encountered.	Pause after 10 Occurrence
8581	DIMM_A2 Correctable ECC error encountered.	Pause after 10 Occurrence
8582	DIMM_A3 Correctable ECC error encountered.	Pause after 10 Occurrence
8583	DIMM_A4 Correctable ECC error encountered.	Pause after 10 Occurrence
8584	DIMM_B1 Correctable ECC error encountered.	Pause after 10 Occurrence
8585	DIMM_B2 Correctable ECC error encountered.	Pause after 10 Occurrence
8586	DIMM_B3 Correctable ECC error encountered.	Pause after 10 Occurrence
8587	DIMM_B4 Correctable ECC error encountered.	Pause after 10 Occurrence
8588	DIMM_C1 Correctable ECC error encountered.	Pause after 10 Occurrence
8589	DIMM_C2 Correctable ECC error encountered.	Pause after 10 Occurrence
858A	DIMM_C3 Correctable ECC error encountered.	Pause after 10 Occurrence
858B	DIMM_C4 Correctable ECC error encountered.	Pause after 10 Occurrence
858C	DIMM_D1 Correctable ECC error encountered.	Pause after 10 Occurrence
858D	DIMM_D2 Correctable ECC error encountered.	Pause after 10 Occurrence
858E	DIMM_D3 Correctable ECC error encountered.	Pause after 10 Occurrence
858F	DIMM_D4 Correctable ECC error encountered.	Pause after 10 Occurrence
85A0	DIMM_A1 Uncorrectable ECC error encountered.	Pause
85A1	DIMM_A2 Uncorrectable ECC error encountered.	Pause
85A2	DIMM_A3 Uncorrectable ECC error encountered.	Pause
85A3	DIMM_A4 Uncorrectable ECC error encountered.	Pause
85A4	DIMM_B1 Uncorrectable ECC error encountered.	Pause

Error Code	Error Message	Response
85A5	DIMM_B2 Uncorrectable ECC error encountered.	Pause
85A6	DIMM_B3 Uncorrectable ECC error encountered.	Pause
85A7	DIMM_B4 Uncorrectable ECC error encountered.	Pause
85A8	DIMM_C1 Uncorrectable ECC error encountered.	Pause
85A9	DIMM_C2 Uncorrectable ECC error encountered.	Pause
85AA	DIMM_C3 Uncorrectable ECC error encountered.	Pause
85AB	DIMM_C4 Uncorrectable ECC error encountered.	Pause
85AC	DIMM_D1 Uncorrectable ECC error encountered.	Pause
85AD	DIMM_D2 Uncorrectable ECC error encountered.	Pause
85AE	DIMM_D3 Uncorrectable ECC error encountered.	Pause
85AF	DIMM_D4 Uncorrectable ECC error encountered.	Pause
8601	Override jumper is set to force boot from lower alternate BIOS bank of flash ROM	No Pause
8602	WatchDog timer expired (secondary BIOS may be bad!)	No Pause
8603	Secondary BIOS checksum fail	No 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
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 an illegal software state error.	Halt
9687	DXE core component encountered an illegal software state error.	Halt
96A7	DXE boot services driver component encountered an illegal software state error.	Halt
96AB	DXE boot services driver component encountered invalid configuration.	No Pause
96E7	SMM driver component encountered an illegal software state error.	Halt
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

POST Error Beep Codes

The following table lists the POST error beep codes. Prior to system video initialization, the BIOS uses these beep codes to inform users on error conditions. The beep code is followed by a user-visible code on the POST Progress LEDs. For complete details, refer to the *Intel® S5500/S5520 Server Board Family BIOS External Product Specification*.

Table 90. POST Error Beep Codes

Beeps	Error Message	POST Progress Code	Description
3	Memory error	0xE8, 0xEB, 0xED, 0xEE	System halted because a fatal error related to the memory was detected.

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

Table 91. Integrated BMC Beep Codes

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

Appendix F: Supported Intel® Server Chassis

The Intel® Server Board S5520UR is supported in the following Intel® rack-mount server chassis:

- Intel® Server Chassis SR2600 URBRP
- Intel® Server Chassis SR2600 URLX
- Intel® Server Chassis SR2625 URBRP
- Intel® Server Chassis SR2625 URLX
- Intel® Server Chassis SR1600 UR
- Intel® Server Chassis SR1600 URSAS
- Intel® Server Chassis SR1625 UR
- Intel® Server Chassis SR1625 URSAS
- Intel® Server Chassis SR2600 URBRPR
- Intel® Server Chassis SR2600 URLXR
- Intel® Server Chassis SR2625 URBRPR
- Intel® Server Chassis SR2625 URLXR
- Intel® Server Chassis SR1600 URR
- Intel® Server Chassis SR1600 URSASR
- Intel® Server Chassis SR1625 URR
- Intel® Server Chassis SR1625 URSASR

The Intel® Server Board S5520URT is supported in the following Intel® rack-mount server chassis:

Intel® Server Chassis SR2625 URLXT

Glossary

This appendix contains important terms used in this document. For ease of use, numeric entries are listed first (e.g., “82460GX”) followed by alpha entries (e.g., “AGP 4x”). Acronyms are followed by non-acronyms.

Term	Definition
ACPI	Advanced Configuration and Power Interface
AP	Application Processor
APIC	Advanced Programmable Interrupt Control
ARP	Address Resolution Protocal
ASIC	Application Specific Integrated Circuit
ASMI	Advanced Server Management Interface
BIOS	Basic Input/Output System
BIST	Built-In Self Test
BMC	Baseboard Management Controller
BPP	Bits per pixel
Bridge	Circuitry connecting one computer bus to another, allowing an agent on one to access the other
BSP	Bootstrap Processor
Byte	8-bit quantity
CBC	Chassis Bridge Controller (A microcontroller connected to one or more other CBCs, together they bridge the IPMB buses of multiple chassis.
CEK	Common Enabling Kit
CHAP	Challenge Handshake Authentication Protocol
CMOS	Complementary Metal-oxide-semiconductor 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.
DHCP	Dynamic Host Configuration Protocal
DPC	Direct Platform Control
EEPROM	Electrically Erasable Programmable Read-Only Memory
EHCI	Enhanced Host Controller Interface
EMP	Emergency Management Port
EPS	External Product Specification
ESB2	Enterprise South Bridge 2
FBD	Fully Buffered DIMM
F MB	Flexible Mother Board
FRB	Fault Resilient Booting
FRU	Field Replaceable Unit
FSB	Front Side Bus
GB	1024 MB
GPA	Guest Physical Address
GPIO	General Purpose I/O
GTL	Gunning Transceiver Logic
HPA	Host Physical Address
HSC	Hot-swap Controller
Hz	Hertz (1 cycle/second)
I^2C	Inter-Integrated Circuit Bus

Term	Definition
IA	Intel® Architecture
IBF	Input Buffer
ICH	I/O Controller Hub
ICMB	Intelligent Chassis Management Bus
IERR	Internal Error
IFB	I/O and Firmware Bridge
ILM	Independent Loading Mechanism
IMC	Integrated Memory Controller
INTR	Interrupt
I/OAT	I/O Acceleration Technology
IOH	I/O Hub
IP	Internet Protocol
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
IR	Infrared
ITP	In-Target Probe
KB	1024 bytes
KCS	Keyboard Controller Style
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Authentication Protocol
LED	Light Emitting Diode
LPC	Low Pin Count
LUN	Logical Unit Number
MAC	Media Access Control
MB	1024 KB
MCH	Memory Controller Hub
MD2	Message Digest 2 – Hashing Algorithm
MD5	Message Digest 5 – Hashing Algorithm – Higher Security
ME	Management Engine
MMU	Memory Management Unit
ms	Milliseconds
MTTR	Memory Type Range Register
Mux	Multiplexor
NIC	Network Interface Controller
NMI	Nonmaskable Interrupt
OBF	Output Buffer
OEM	Original Equipment Manufacturer
Ohm	Unit of electrical resistance
OVP	Over-voltage Protection
PECI	Platform Environment Control Interface
PEF	Platform Event Filtering
PEP	Platform Event Paging
PIA	Platform Information Area (This feature configures the firmware for the platform hardware)

Term	Definition
PLD	Programmable Logic Device
PMI	Platform Management Interrupt
POST	Power-On Self Test
PSMI	Power Supply Management Interface
PWM	Pulse-Width Modulation
QPI	QuickPath Interconnect
RAM	Random Access Memory
RASUM	Reliability, Availability, Serviceability, Usability, and Manageability
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)
SDR	Sensor Data Record
SECC	Single Edge Connector Cartridge
SEEPROM	Serial Electrically Erasable Programmable Read-Only Memory
SEL	System Event Log
SIO	Server Input/Output
SMBUS	System Management BUS
SMI	Server Management Interrupt (SMI is the highest priority non-maskable interrupt)
SMM	Server Management Mode
SMS	Server Management Software
SNMP	Simple Network Management Protocol
SPS	Server Platform Services
SSE2	Streaming SIMD Extensions 2
SSE3	Streaming SIMD Extensions 3
SSE4	Streaming SIMD Extensions 4
TBD	To Be Determined
TDP	Thermal Design Power
TIM	Thermal Interface Material
UART	Universal Asynchronous Receiver/Transmitter
UDP	User Datagram Protocol
UHCI	Universal Host Controller Interface
URS	Unified Retention System
UTC	Universal time coordinare
VID	Voltage Identification
VRD	Voltage Regulator Down
VT	Virtualization Technology
Word	16-bit quantity
WS-MAN	Web Services for Management
ZIF	Zero Insertion Force

Reference Documents

See the following documents for additional information:

- *Intel® S5500/S5520 Server Board Family BIOS External Product Specification*
- *Intel® Server System Integrated Baseboard Management Controller Core External Product Specification*
- *Intel® 5500/5520 Chipset I/O Controller Hub External Design Specification*