Intel® Server Board Set SE8501HW4

Technical Product Specification

Intel order number: D24295-001

Revision 1.0

October, 2005

Enterprise Platforms and Services – Marketing

Revision History

Date	Revision Number	Modifications
August 2005	0.5	Initial release.
October 2005	1.0	Production Release

Disclaimers

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, 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.

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

The IntelP®P Server Board Set SE8501HW4 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 baseboards contain a number of high-density VLSI and power delivery components that need adequate airflow to cool. Intel’s own chassis are designed and tested to meet the intended thermal requirements of these components when the fully integrated system is used together. It is the responsibility of the system integrator that chooses not to use Intel developed server building blocks to consult vendor datasheets and operating parameters to determine the amount of air flow required for their specific application and environmental conditions. Intel Corporation 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, Xeon®, Itanium®, and XScale® are trademarks or registered trademarks of Intel Corporation.

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

Table of Contents

List of Figures

List of Tables

< This page intentionally left blank. >

1. Product Overview

The Intel® Server Board Set SE8501HW4 is an improvement to the fourth generation of four-way IA-32 server boards. The board set uses the Intel® E8501 Chipset, and the next generation of memory and processor technologies. This product diverges from other Intel server boards and platforms in the following ways:

- Addition of PCI Express* technology
- Addition of Double Data Rate Two (DDR2) memory
- Memory implemented across up to four memory boards, with enhanced performance and reliability features
- Optional mass storage expansion for Fibre Channel and RAID
- Up to four processors operating on an 800MTS Front Side Bus (FSB)
- Support for Hyper-Threading Technology (HT Technology) and dual core processors for up to 16 logical processors
- Removal of IDE, floppy, and PS/2* ports

The Intel® Server Board Set SE8501HW4 supports up to four 64-bit Intel® Xeon® processors MP with up to 8MB L3 cache and incorporates features that clearly differentiate it as a high availability server. Building on previous server platforms, the Intel® Server Board Set SE8501HW4 introduces redundant memory, networking, and the BIOS flash in addition to the enterprise features of hot-swap PCI slots, standards-based server management, and server-oriented embedded I/O. Remote monitoring and management features are also included, providing a new level of user tools for server administration.

The Intel® Server Board Set SE8501HW4 consists of two primary boards: main and memory. Up to four memory boards plug vertically into the mainboard. The board set was designed to work with the Intel® Server Platform SR4850HW4/M, a 4U chassis, and the Intel® Server Platform SR6850HW4/M, a 6U chassis. The board set may also be used in a non-Intel chassis that meets the power and cooling requirements found in this specification. Please refer to the *Intel® Server Platform SR4850HW4/M External Product Specification* and *Intel® Server Platform SR6850HW4/M External Product Specification* for more information on these products.

This document describes the mainboard and memory board components of the Intel® Server Board Set SE8501HW4.

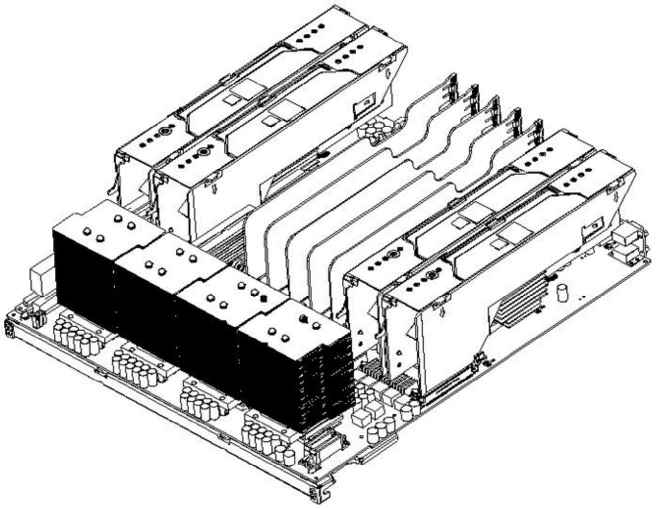


Figure 1. Intel® Server Board Set SE8501HW4, Populated

1.1 Intel® Server Board Set SE8501HW4 Functional Changes

The Intel® Server Board Set SE8501HW4 has been functionally improved over the previous product to include support for the following:

- 64-bit Intel® Xeon® processors 7000 sequence (up to 4 physical and 16 logical processors)
- Improved FSB bandwidth up to 800 MTS or 6.4 GB theoretical max throughput per bus
- Real-Time Clock (RTC) access added to the Baseboard Management Controller (BMC)

1.2 Board Set Features

This section discusses the features for the Intel® Server Board Set SE8501HW4, which includes:

- Up to four 64-bit Intel® Xeon® processors MP with up to 8MB L3 cache, including support for 64-bit Intel® Xeon® processors 7000 sequence.
- Intel® E8501 Chipset:
    1. Intel® E8501 Chipset North Bridge (NB): provides two processor buses and connection to I/O and memory subsystems
    2. Intel® E8501 Chipset eXtended Memory Bridge (XMB): provides hot-plug support for up to 64GB of DDR2 memory
    3. Intel® 6700 PXH 64-bit PCI Hub: provides support for PCI-X* I/O

4. Intel® IOP332 Storage I/O Processor : provides support for PCI-X* adapters and contains Intel XScale® technology to support optional RAID-on-MotherBoard (ROMB)
5. Intel® 81801EB I/O Controller Hub 5 (ICH5): provides support for the system BIOS, video, USB 2.0, and Serial ATA (SATA).

- Advanced I/O slots including PCI Express* and PCI-X* and support circuits:

6. One hot-plug PCI Express* x8 slot
7. Three hot-plug PCI Express* x4 slots
8. One hot-plug 64-bit PCI-X* 133MHz, 1.0 slot
9. Two 64-bit PCI-X* 100MHz, 1.0 slots (not hot-plug)

- Server management with either the Intel® Management Module - Professional Edition or Intel® Management Module - Advanced Edition
- ATI* Radeon* 7000 video controller, with 16MB SDRAM
- Broadcom* BCM5704C NetXtreme Gigabit Ethernet controller provides two ports on the rear of the mainboard
- LSI Logic* 53C1030 Ultra320* SCSI controller provides two independent Ultra320* SCSI interfaces
- Optional ROMB support provides two channels of RAID 0, 1, 5, 10 or 50
- Optional custom Intel® Fibre Channel Module: provides two 2Gbps optical connectors

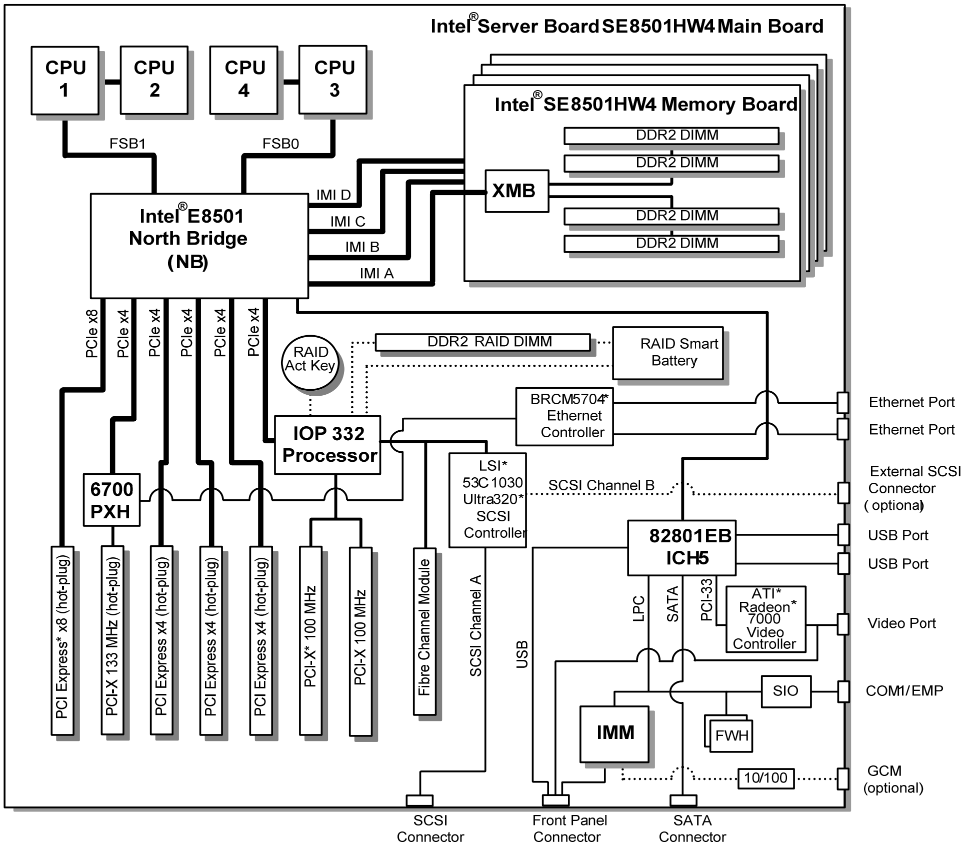


Figure 2. Intel® Server Board Set SE8501HW4 Interconnect Diagram

2. Processor and Chipset

2.1 Processors Supported

The Intel® Server Board Set SE8501HW4 supports 64-bit Intel® Xeon® processors MP, which are based on the Intel NetBurst® microarchitecture. Several architectural and microarchitectural enhancements have been added to this processor, including an increased L2 cache size and for some models, an integrated L3 cache. Table 1 provides a feature set overview of the 64-bit Intel® Xeon® processors MP.

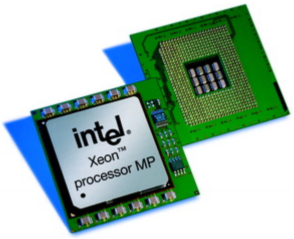


Figure 3. 64-bit Intel® Xeon® Processors MP

Table 1. Processor Feature Overview

Feature	64-bit Intel® Xeon® processors MP with 1MB L2 cache	64-bit Intel® Xeon® processors MP with up to 8MB L3 cache	64-bit Intel® Xeon® processors 7000 sequence
Package	FC-mPGA4		
L2 cache size	1MB		2MB per core
L3 cache size	N/A	4MB or 8MB	N/A
Core operating voltage	1.0975 to 1.4V	1.171 to 1.3250V	1.2875 to 1.4125 V
Cache operating voltage	N/A	1.1 to 1.25V	N/A
Front side bus	667MTS with data-bus Error Correcting Code (ECC), bandwidth up to 5.33GB/s		800MTS with ECC, bandwidth up to 6.4GB/s

The 64-bit Intel® Xeon® processors MP include the following advanced features:

- Intel® Extended Memory 64 Technology (Intel® EM64T) for executing both 32-bit and 64-bit applications simultaneously
- Hyper-Threading (HT Technology) providing two logical processors
- Intel® Demand-Based Switching (DBS) for power savings
- 64-bit Intel® Xeon® processors 7000 sequence dual core support
- Execute-Disable Bit for hardware support of security features
- Quad-channel DDR2 400MHz memory support
- PCI Express* for faster serial interconnects
- Streaming Single Instruction, Multiple Data (SIMD) Extensions 2 and 3 (SSE2, SSE3)

For more information, please refer to the following:

- 64-bit Intel® Xeon® processors MP with 1MB L2 cache Datasheet
- 64-bit Intel® Xeon® processors MP with up to 8MB L3 cache Datasheet
- 64-bit Intel® Xeon® processors MP with 1MB L2 cache Specification Update
- 64-bit Intel® Xeon® processors MP with up to 8MB L3 cache Specification Update

2.2 Heat Sink

The Intel® Server Board Set SE8501HW4 uses the reference design Common Enabling Kit (CEK) heat sinks, which meet the 64-bit Intel® Xeon® processors MP thermal performance targets. Each CEK heat sink consists of the following components:

- Passive heat sink (with captive standoff and screws)
- Thermal Interface Material (TIM-2) – to cover the entire processor Integrated Heat Spreader (IHS) and the heat sink base
- Hat spring – mounted below the Intel® Server Board Set SE8501HW4 mainboard

2.3 Processor and VRM Installation Order

The Intel® Server Board Set SE8501HW4 mainboard includes a single integrated cache Voltage Regulator Down (VRD) for 64-bit Intel® Xeon® processors with an L3 integrated cache on processor sockets 1 and 2. Additionally, the Intel® Server Board Set SE8501HW4 mainboard includes two integrated core Voltage Regulators Down (VRD) for supported Intel® Xeon® processors on processor sockets 1 and 2. Installing a processor in sockets 3 and 4 requires a core Voltage Regulator Module (VRM) for each socket and, when using a processor with L3 cache, one L3 Cache VRM.

Some processor signals do not have on-die termination and must be terminated at an end agent. The Intel® Server Board Set SE8501HW4 mainboard was designed with two separate Front Side Buses (FSBs). For each bus with a processor installed, the first socket on that bus must be used to ensure proper signal termination. A processor must be installed in socket 1 before socket 2, and socket 3 before socket 4. Refer to Table 2 for the processor installation order.

Table 2. Processor Installation Order

Number of Processors	Sockets				L3 Cache VRM9DO J1H2[2]	Core VRM J1F1	Core VRM J3F1
	1	2	3	4			
One	Installed						
			Installed		Installed[2]	Installed	
Two[1]	Installed	Installed					
	Installed		Installed		Installed[2]	Installed	
Three[1]	Installed	Installed	Installed		Installed[2]	Installed	
	Installed		Installed	Installed	Installed[2]	Installed	Installed
Four	Installed	Installed	Installed	Installed	Installed[2]	Installed	Installed

Table 3. VRM Installation Order

VRM Type		64-bit Intel® Xeon® Processors MP with 1MB L2 Cache	64-bit Intel® Xeon® Processors MP with up to 8MB L3 Cache	64-bit Intel® Xeon® Processors 7000 Sequence
Cache VRM	VRM 9.1	Does Not Boot	Does Not Boot	Does Not Boot
	L3 Cache VRM9DO		Supported[2]	
Core VRM	10.2LD VRM	Supported	Supported	
	10.2 VRM	Supported	Supported	Supported

1. There is no performance gained by splitting the processors across the FSBs. Intel has validated sequential process installation, with a one-processor configuration using socket 1; a two-processor configuration using sockets 1 and 2; and a three-processor configuration using sockets 1, 2, and 3.

2. The L3 Cache VRM9DO is required when installing 64-bit Intel® Xeon® processors MP with L3 cache in socket 3 or 4.

2.4 Intel® E8501 Chipset

The Intel® E8501 Chipset is the highest performance, most scalable platform offering in the 64-bit Intel® Xeon® processor MP family. The chipset represents an improvement to Intel's four-way multi-processor platform. It is designed for multi-core processors, and includes the following advanced features:

- Support for up to four 64-bit Intel® Xeon® processors FSB operating at 800 MTS
- Maintains coherency across both buses
- Double-pumped 40-bit address buses with a total address bandwidth of 200 million addresses/second
- Quad-pumped, 64-bit data bus providing a bandwidth of 6.4 GB/s per bus
- x8 Single Device Data Correction (x8 SDDC) technology for memory error correction
- Hardware memory initialization
- ECC protection on data signals and parity protection on address signals
- Support for hot-plug memory and performance operations

This section provides an overview of the chipset components, for more detailed information refer to the *Intel® E8501 Chipset Datasheets* referenced in the Appendix.

2.4.1 North Bridge (NB)

The Intel® E8501 Chipset North Bridge (NB) is the center of the system architecture and provides interconnection to the following:

- Up to four 64-bit Intel® Xeon® processors via two 800 MTS FSBs optimized for server applications
- Up to 64GB memory via four Independent Memory Interfaces (IMI)
- I/O subsystem components via one PCI Express* and the Intel® 82801EB I/O Controller Hub 5 (ICH5)

2.4.2 eXtended Memory Bridge (XMB)

The Intel® E8500 Chipset eXtended Memory Bridge (XMB) provides interface between the NB and DDR2 400MHz DIMMs. The Intel® Server Board Set SE8501HW4 includes up to four memory boards, each with an XMB and four DDR2 400MHz DIMM locations.

2.4.3 Intel® IOP332 Storage I/O Processor

The Intel® IOP332 Storage I/O Processor contains a PCI Express* to PCI-X* bridge and performs bridging functions between the PCI Express* interface of the NB and PCI-X* devices The Intel® Server Board Set SE8501HW4 contains one Intel® IOP332 Storage I/O Processor that has two PCI bus interfaces, which provide:

- Slots 6 and 7 (PCI-X* 100MHz, non-Hot-Plug)
- LSI Logic* 53C1030 Ultra320* SCSI controller
- Intel® Fibre Channel Module connector

2.4.4 Intel® 82801EB I/O Controller Hub 5 (ICH5)

The Intel® 82801EB I/O Controller Hub 5 (ICH5) provides a hub interface-to-PCI bridge, PCI-to-LPC bridge, and Legacy I/O controllers. Some of the features of the ICH5 are not used in this board set. The Intel® Server Board Set SE8501HW4 contains one ICH5, which provides:

- Integrated Serial ATA (SATA) controller
- High-speed USB 2.0 host controller
- ATI* Radeon* 7000 video controller
- Support for System Management Bus (SMBus) specification, version 2.0 and I^2C
- ACPI power management logic support
- Firmware Hub (FWH) interface support

2.4.5 Intel® 6700 PXH 64-bit Hub (PXH)

The Intel® 6700 PXH 64-bit Hub performs bridging functions between the PCI Express* interface of the NB and PCI-X* devices. The Intel® Server Board Set SE8501HW4 contains one PXH that has two PCI bus interfaces, which provide:

- Slot 2 (PCI-X* 133Mhz Hot-Plug)
- Broadcom* BCM5704C dual channel Gigabit Ethernet controller

3. I/O Subsystems

3.1 PCI Subsystem

The PCI subsystem consists of eight slots, seven available to standard PCI adapters and one for the Intel® Server Board Set SE8501HW4-specific Intel® Fibre Channel Module.

Table 4. PCI Expansion Slot Features

Segment	Slot	Hot-Plug	Technology	Width	Bandwidth (GB/s)
North Bridge (C)	1	Yes	PCI Express*	x8	4
PXH (A)	2	Yes	PCI-X* 133	64-bit	1
North Bridge (D)	3	Yes	PCI Express*	x4	2
North Bridge (B)	4	Yes	PCI Express*	x4	2
North Bridge (B)	5	Yes	PCI Express*	x4	2
Intel® IOP332 Storage I/O Processor (B)	6	No	PCI-X* 100	64-bit	0.8
Intel® IOP332 Storage I/O Processor (B)	7	No	PCI-X* 100	64-bit	0.8
Intel® IOP332 Storage I/O Processor (A)	Fibre Channel	No	PCI-X* 100	64-bit	0.8

3.1.1 PCI Interrupts

PCI Express* interrupts are delivered in-band over the PCI Express* bus via the Message Signal Interrupt (MSI) mechanism.

PCI and PCI-X* devices can deliver interrupts either by asserting IRQ signals that are routed to the PXH or Intel® IOP332 Storage I/O Processor IOxAPIC, or over the PCI-X* bus via MSI. In either case, the PXH and/or Intel® IOP332 Storage I/O Processor forward the interrupt to the NB as an Inbound Write for the processor to handle the event.

Table 5 describes how the interrupts for each of the PCI devices are mapped to the PXH and Intel® IOP332 Storage I/O Processor.

Table 5. PCI Interrupt Mapping

Device	APIC	INTA#	INTB#	INTC#	INTD#
Broadcom* BCM5704	PXH (B)	PX2B_IRQ0_N	PX2B_IRQ1_N		
Slot 2	PXH (A)	PX2A_IRQ0_N	PX2A_IRQ1_N	PX2A_IRQ2_N	PX2A_IRQ3_N
Slot 6	Intel® IOP332 Storage I/O Processor (B)	PX1B_XINT4_N	PX1B_XINT5_N	PX1B_XINT6_N	PX1B_XINT7_N
Slot 7	Intel® IOP332 Storage I/O Processor (B)	PX1B_XINT6_N	PX1B_XINT7_N	PX1B_XINT4_N	PX1B_XINT5_N

Device	APIC	INTA#	INTB#	INTC#	INTD#
LSI Logic* 53C1030	Intel® IOP332 Storage I/O Processor (A)	PX1A_XINT0_N	PX1A_XINT1_N	-	-
Intel® Fibre Channel Module	Intel® IOP332 Storage I/O Processor (A)	PX1A_XINT2_N	PX1A_XINT3_N	-	-

3.1.2 PCI IDSEL Signal

The IDSEL signal is used as a chip-select for devices during read and write transactions. The PXH and Intel® IOP332 Storage I/O Processor assert a specific address bit on a given PCI bus to toggle the IDSEL signal to the PCI device. For the Intel® Server Board Set SE8501HW4 mainboard the address bit to IDSEL mapping is shown in Table 6.

Table 6. IDSEL Mapping

Device	Device #	IDSEL	Host Bridge
Broadcom* BCM5704	2	PX2B_AD<18>	PXH (B)
Slot 2	2	PX2A_AD<18>	PXH (A)
Slot 6	6	PX1B_AD<22>	Intel® IOP332 Storage I/O Processor (B)
Slot 7	7	PX1B_AD<23>	Intel® IOP332 Storage I/O Processor (B)
LSI Logic* 53C1030	5	PX1A_AD<21>	Intel® IOP332 Storage I/O Processor (A)
Intel® Fibre Channel Module	15	PX1A_AD<31>	Intel® IOP332 Storage I/O Processor (A)
ROMB enabled on Intel IOP332 Storage I/O Processor	14	N/A	Internal to Intel® IOP332 Storage I/O Processor

Note: When the ROMB solution is enabled, the IDSEL to the LSI Logic* 53C1030 is inhibited by the Intel® IOP332 Storage I/O Processor. This effectively hides the SCSI controller from the system and the Intel® IOP332 Storage I/O Processor acts as the SCSI (or RAID) controller. Since the Intel® Fibre Channel Module is attached to the same bus as the SCSI controller, the Intel® Fibre Channel Module is set to device 15 so that it is not affected by the device hiding operation required for the ROMB solution.

3.1.3 Bus Arbitration Signals

Request (REQ#) signals indicate to the bus arbiter that an agent/device desires the use of the bus. The Grant (GNT#) signal indicates to the agent/device that access to the bus has been granted. Every master has its own REQ#, which must be tri-stated while RST# is asserted. These are point-to-point signals, which are assigned to every bus master.

In the Intel® Server Board Set SE8501HW4, there is one arbiter for each PCI bus on the PXH and Intel® IOP332 Storage I/O Processor. The PXH contains an arbiter for slot 2 and the BCM5704 and the Intel® IOP332 Storage I/O Processor contains an arbiter for slots 6 and 7, LSI Logic* 53C1030, and the Intel® Fibre Channel Module.

Table 7. Arbitration Connections

Device	REQ#	GNT#	Host Bridge
Broadcom* BCM5704	PX2B_REQ0_N	PX2B_GNT0_N	PXH (B)
Slot 2	PX2A_REQ0_N	PX2A_GNT0_N	PXH (A)
Slot 6	PX1B_REQ1_N	PX1B_GNT1_N	Intel® IOP332 Storage I/O Processor (B)
Slot 7	PX1B_REQ0_N	PX1B_GNT0_N	Intel® IOP332 Storage I/O Processor (B)
LSI Logic* 53C1030	PX1A_REQ0_N	PX1A_GNT0_N	Intel® IOP332 Storage I/O Processor (A)
Intel® Fibre Channel Module	PX1A_REQ1_N	PX1A_GNT1_N	Intel® IOP332 Storage I/O Processor (A)

3.1.4 Wake On LAN

Wake On LAN (WOL) is supported on the Intel® Server Board Set SE8501HW4 either from PCI devices through the PME# signal, or PCI Express* via the WAKE# signal.

Any PCI Express* adapter can generate a wake event by asserting the WAKE# signal. This signal is OR'd to all other PCI Express* WAKE# signals and routed to the ICH5 after being qualified with intrusion and a prior graceful shutdown. The assertion of a WAKE# signal causes the system to return to the ACPI S0 sleep state. Once system power is up and the PCI Express* devices are configured, a PME message is sent to the NB identifying the device that woke the system.

For all the PCI devices or the Ethernet controller, PME# is handled similarly to the PCI Express* WAKE# signal. All PME# signals are OR'd together and routed to the ICH5 after being qualified with intrusion and a prior graceful shutdown. The PME assertion wakes the system but does not generate an interrupt from the ICH5. Once the system is powered up, the PXH or Intel® IOP332 Storage I/O Processor generates a PME interrupt message to the operating system. The operating system determines which slot is the PME source by polling the PXH and Intel® IOP332 Storage I/O Processor.

3.1.5 PCI Hot-Plug Support

PCI Hot-Plug is the concept of removing a standard PCI adapter card from a system without stopping the software or powering down the system as a whole.

In the Intel® Server Board Set SE8501HW4, PCI Slot 2 supports the *PCI Hot-Plug Specification, Revision 1.1.* It is configured to insure the PXH isolates the slot from the PCI bus when no adapter is present. The four PCI Express* slots support the *PCI Express Base Specification, Revision 1.0a*.

3.1.5.1 Hardware Components

The Intel® Server Board Set SE8501HW4 contains buttons and LEDs to assist a user for hot-plug operations. Buttons provide isolation circuitry to physically disconnect the hot-plug adapter from the PCI buses while LEDs provide slot power and status. The LEDs have enough luminous intensity to pass through system-level light pipes and be visible at the top of a system. An attention button can be used to invoke a hot-plug sequence to remove or add an adapter without the use of an operating system/software interface.

Table 8. PCI Hot-Plug LEDs

LED	State	Meaning
Power (green)	Off	Power off: All main rails have been removed from slot. Card can be inserted or removed.
	On	Power on: Slot is powered on. Card cannot be inserted or removed.
	Blinking	Power transition: Slot is in the process of changing state. Card cannot be inserted or removed.
Attention (amber)	Off	Normal: Normal operation.
	On	Attention: Power fault or operational problem at this slot.
	Blinking	Locate: Slot is being identified at the user's request.

3.1.5.2 Software Components

PCI Hot-Plug operations are supported by the system BIOS, an operating system driver and an optional operating system administrative interface. The Intel® Server Board Set SE8501HW4 BIOS provides the following:

- Initialization of the hot-plug hardware components
- Logging of hot-plug events through server management
- ACPI table generation

Microsoft Windows Server 2003, Enterprise Edition* includes support for PCI Hot-Plug through the taskbar "Unplug or Eject Hardware" interface but may require an updated adapter device driver. Refer to other operating systems' manuals for more information on how to perform hot-plug operations. Reference the PCI adapter release notes for specific information on support and driver requirements.

3.1.5.3 Hot Removal Example

3.1.5.3.1 Under Microsoft Windows Server 2003, Enterprise Edition:*

1. Open the cover of the system to access the adapters and status LEDs.
2. Double-click "Unplug/Eject" in the taskbar to open the "Unplug or Eject Hardware" menu.
3. Select the device to be removed and click "Stop".
4. Wait for the power LED to turn off.
5. Disengage rocker, retention, and/or safety devices.
6. Remove the adapter.

3.1.5.3.2 Under other operating systems:

1. Open the cover of the system to access the adapters and status LEDs.
2. Press the attention button for the slot. (Press the attention button within five seconds to abort the hot-plug operation.)
3. Wait for the power LED to turn off.
4. Disengage rocker, retention, and/or safety devices.
5. Remove the adapter.

3.1.5.4 Hot Addition Example

3.1.5.4.1 Under Microsoft Windows Server 2003, Enterprise Edition:*

1. Open the cover of the system to access adapters and view the status LEDs.
2. Install the adapter into the slot.
3. Engage rocker, retention, and/or safety devices.
4. Wait for the software user interface to open. Confirm the device to be enabled.
5. Wait for the power LED to turn on.

Note: If the attention LED is blinking, a power fault has occurred. The user may need to remove the adapter; wait for the LED to turn off, and re-start the hot add operation.

3.1.5.4.2 Under other operating systems:

1. Open the cover of the system to access adapters and view the status LEDs.
2. Install the adapter into the slot.
3. Engage rocker, retention, and/or safety devices.
4. Press the attention button for the slot. (Press the attention button within five seconds to abort the hot-plug operation.)
5. Wait for the power LED to turn on.
6. Enable the device in your operating system.

Note: If the attention LED is blinking, a power fault has occurred. The user may need to remove the adapter; wait for the LED to turn off, and re-start the hot add operation.

3.2 Ultra320* SCSI Subsystem

A single LSI Logic* 53C1030 controller provides the onboard Ultra320* SCSI interface. The controller resides on the PCI Bus Segment A (PX1A), off the Intel® IOP332 Storage I/O Processor. For optimal performance, the controller is configured as a 64-bit PCI-X* 100MHz device.

The LSI Logic 53C1030 supports two Ultra320* SCSI channels, both validated for LVDS operation. In the Intel Server Platform SR4850HW4/M, the first channel is routed to the internal hot-swap hard disk drive bay and the second is optionally connected to an external connector. In the Intel Server Platform SR6850HW4/M, both channels are routed to the internal hot-swap hard disk drive bay. Intel has not validated Single Ended (SE) operation for this device.

The Intel® Server Board Set SE8501HW4 mainboard provides active terminators, termination voltage, auto re-sealable fuse, and protection diode for both SCSI channels. The SCSI ROM allows for the configuration of onboard termination.

PCI Express* and PCI-X* adapter cards based on a LSI Logic* 53C1030 controller should have the option ROM for the slot turned off in the system BIOS setup. This allows the embedded LSI Logic 53C1030 controller firmware to manage the add-in adapters. The Intel® Server Board Set SE8501HW4 mainboard does not have a physical flash device, so the system BIOS loads the required RISC F/W into the embedded LSI Logic* 53C1030 controller during POST. A 53C1030-based adapter cannot take control of the embedded SCSI controller since those cards do not have the required RISC F/W to start the embedded SCSI device. Starting with the LSI Logic* Fusion-MPT SCSI BIOS 5.10.02, the embedded LSI Logic* 53C1030 SCSI controller can control additional LSI Logic* 53C1030-based adapter cards.

3.3 Intel® RAID-on-MotherBoard (ROMB)

The Intel® IOP332 Storage I/O Processor, in conjunction with the LSI Logic* 53C1030, provides an optional RAID-on-MotherBoard (ROMB) solution which supports RAID levels 0, 1, 5, 10, and 50. A 2MB flash component and a non-volatile SRAM store the code and hardware configuration information.

To activate the ROMB solution, a physical Intel® RAID Activation Key and DDR2 400MHz RAID DIMM must be installed on the Intel® Server Board Set SE8501HW4 mainboard. The Intel® RAID Activation Key contains a registration code required to unlock the LSI* Mega RAID Controller Memory solution. The DDR2 400MHz RAID DIMM serves as memory for the Intel® IOP332 Storage I/O Processor and a disk cache to store write data for the drives. In addition to these components, an Intel® RAID Smart Battery may also be installed to refresh the RAID DIMM when system power drops below specifications.

After installing an Intel® RAID Activation Key and DDR2 400MHz RAID DIMM, and optional Intel® RAID Smart Battery, the system BIOS setup allows the user to enable the ROMB solution. During option ROM scan, an option to configure the RAID is displayed. The following three sections provide an overview of the Intel ROMB solution.

3.3.1 Intel® RAID Activation Key

The Intel® RAID Activation Key is a round one-wire serial EEPROM device programmed by Intel. This key has a registration code required to enable the LSI* Mega RAID solution.

3.3.2 DDR2 RAID DIMM

The ROMB solution only supports 400MHz registered ECC, with a CAS latency of four clock cycles. Please refer to the *Intel® Server Board SE8500HW4 Memory Qualification List* for supported memory.

3.3.3 Intel® RAID Smart Battery

The Intel® RAID Smart Battery keeps the contents of the DDR2 400MHz RAID DIMM preserved if power drops below specifications. When the Intel® IOP332 Storage I/O Processor senses power has dropped below specifications, it initiates a power fail sequence that safely puts the RAID DIMM into self-refresh state. The power subsystem generates enough of a delay to allow the Intel® IOP332 Storage I/O Processor to complete its power fail sequence, even in the event of total system power loss. After the power fail sequence is completed, additional logic keeps the RAID DIMM in self-refresh mode. When power is restored, data from the RAID DIMM is safely written to the disk array.

3.4 Gigabit Ethernet

A single Broadcom* BCM5704C controller provides the onboard Gigabit Ethernet interface. This controller has two ports that can independently operate at 1000/100/10 Mbps and support failover and teaming for greater reliability and performance. The two media access controllers support full-duplex and half-duplex modes at all speeds and have their own PCI configuration space and on-chip memory for higher performance with load balancing and packet buffering. For optimal performance, the controller is configured as a 64-bit PCI-X* 133MHz device. The ICH5 contains an Ethernet controller, but this device is not used by the Intel® Server Board Set SE8501HW4.

3.5 Serial ATA (SATA)

The ICH5 provides a Serial ATA (SATA) interface with a transfer rate of up to 1.5GB/s. The Server Board Set SE8501HW4 mainboard has a standard 7-pin vertical connector for this feature. SATA cables should be 1 meter (40 inches) or less in length.

3.6 Fibre Channel

The Intel® Fibre Channel Module is attached to the Intel® IOP332 Storage I/O Processor via a custom-wired PCI Express* x16 slot on the Intel® Server Board Set SE8501HW4 mainboard. The module uses a Qlogic* ISP2322 FC-PCI-X* controller and has the following features:

- Two independent 2 Gbps Fibre Channel ports
- Support for Fibre Channel virtual interface (VI) protocol
- Automatically negotiates Fibre Channel bit rate (1 or 2 Gbps)
- Supports up to 400 MBps sustained Fibre Channel data transfer rate
- 1 MB SRAM per port
- Data and code parity protection
- Host intervention not required to execute complete SCSI, IP, or VI operations
- LC-style optical connectors
- Works with the Qlogic* SANsurfer Management Suite and other Qlogic* FC cards

For more information, please refer to the *Intel® Fibre Channel Module User Guide*.

3.7 Firmware Hubs

The Intel Server Board Set SE8500HW4 mainboard has a combined total of 4MB flash memory that serves as the firmware hub (FWH) for the system BIOS. The system BIOS fits into 2MB of flash; the rolling BIOS feature utilizes two BIOS images of 2MB each for a total of 4MB. See Section 5 for more information on the rolling BIOS.

3.8 Video

A single ATI* Radeon* 7000 video controller provides the onboard video interface. The ATI* Radeon* 7000 features the following technologies:

- 2D/3D video accelerator
- Dual DAC for integrated, cost-effective multi-panel support
- Resolutions from VGA up to UXGA (1600x1200)
- 16MB SDRAM video memory
- 32-bit/33MHz PCI host interface

Using the default operating system video driver options, the VGA signal is mirrored between the rear panel and the front panel connector. This design consideration was made to facilitate user debug of an operating system hard failure. When the system is in a failure state, a portable monitor can be attached to the front of the system to assist in the determination of root cause. Since this is an enterprise server, Intel has not validated the video driver configured with the front panel I/O board VGA connector in a non-mirrored, extended desktop, state.

3.9 USB 2.0

The ICH5 provides four USB 2.0 interfaces. The interfaces are as follows:

- One internal connector on the Intel® Server Board Set SE8501HW4 mainboard
- A dual-stack USB connector on the rear panel
- One interface routed to the front panel connector.

3.10 Serial

The SIO provides two RS232 serial communication ports (COM1 and COM2). COM1 is provided through DB9 connector on the rear panel of the Intel® Server Board Set SE8501HW4 mainboard. COM2 is internal to the chassis and available as an unshielded 9-pin header (2 x 5, with pin 10 removed for keying). COM1 is available as an Emergency Management Port (EMP) for remote server management, and when used in this mode, it is unavailable to the BIOS/operating system. When server management is setup for Serial Over LAN (SOL) remote server management, COM2 is also unavailable to the BIOS/operating system.

4. Intel® Server Board Set SE8501HW4 Memory Board

One to four Intel® Server Board Set SE8501HW4 memory boards plug vertically into the Intel® Server Board Set SE8501HW4 mainboard. The memory board has the following features:

- Intel® E8501 Chipset eXtended Memory Bridge (XMB)
- Top label 667/800 markings to distinguish new memory board from previous model.
- Two DDR2 400MT/s buses
- Four 240-pin DDR2 400Mhz registered ECC DIMM sockets
- Support for both single-rank and dual-rank DIMMs
- Independent Memory Interface (IMI), a high-speed differential bus
- PCI Express* x16 card edge connector that plugs into the Intel® Server Board Set SE8501HW4 mainboard
- LED error indicators for each DIMM and an attention LED for hot-plug events
- LED indicator for both memory mirroring and RAID configurations
- Memory hot-plug at the card level, based on the PCI Hot-Plug model
- On board power converters for 0.9V, 1.5V, and 1.8V
- Field Replaceable Unit (FRU) device
- Two temperature sensors
- Safety mechanism for instant power shut-down to the memory board

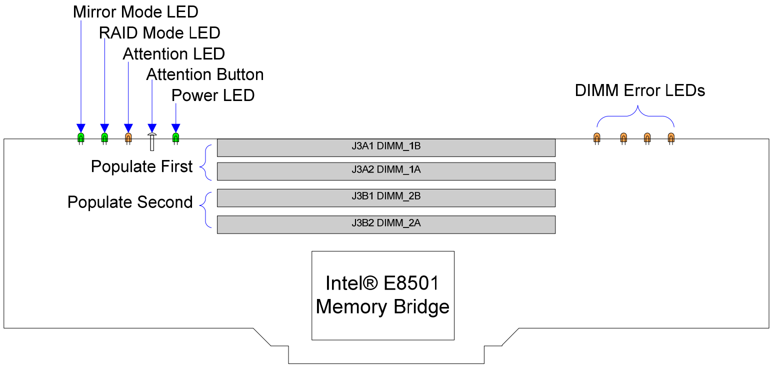


Figure 4. Memory Board Outline Diagram

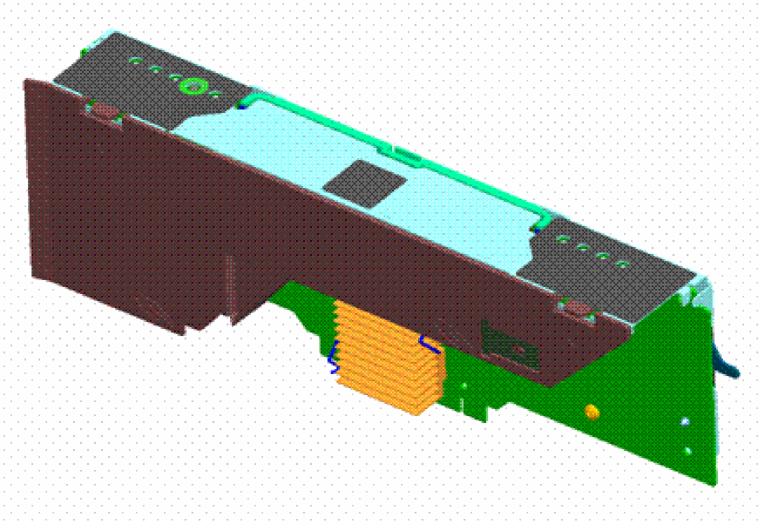


Figure 5. Memory Board Component Diagram

4.1 DDR2 DIMM Support

DDR2 memory offers an effective doubling of the clock rate over DDR memory since data transfers happen on both the rising and falling edge of the clock (double pumped). Due to the lower clock frequency, and improved manufacturing technology, a significant power savings can be achieved, especially when the data bus is not active.

The Intel® Server Board Set SE8501HW4 memory board supports DDR2 400MHz (also referred to as PC2-3200) registered ECC SDRAM with On Die Termination (ODT). Both single-rank and dual-rank technologies are supported, however unbuffered and non-ECC does not function in the Intel® Server Board Set SE8501HW4. Within a single bank, both DIMMs must be identical. (The DIMMs must be identical in size and in the number of devices on the DIMM.)

Speeds less than DDR2 400MHz may be used, but performance is reduced. Intel has only validated DDR2 400MHz SDRAM for specific memory parts; refer to the *Intel® Server Board Set SE8500HW4 Board Memory Qualification List.*

4.2 Installation Order

When only using two memory DIMMs, the first pair of sockets, DIMM_1A and DIMM_1B, must be populated. When using a mixture of single-rank and dual-rank memory DIMMs on one memory board, the dual-rank DIMMs must be installed in the first pair of sockets.

4.3 Memory Initialization

The XMB provides hardware memory initialization. The initialization engine performs two passes. On the first pass, it writes the entire segment. On the second pass, it reads and tests the entire segment. Any errors are logged with the failing DIMM being flagged for BIOS.

4.4 Data Correction and Scrubbing

The XMB employs a Single Device Data Correction (x8 SDDC) algorithm for the memory subsystem that recovers from a component failure during read and write transactions. This corrects and logs a correctable memory error, and logs uncorrectable memory errors.

A patrol scrub can be turned on in the system BIOS that scrubs roughly 64GB of memory behind each XMB every day. The patrol scrub confirms the data for one cache line every 16k core cycles and then increments the address one cache line. During patrol scrub, an erroneous read is logged and re-read. If the re-read is correctable, it is corrected (scrubbed) in memory. A conflicting read or write request-pending issue is held until the scrub is finished.

4.5 Memory Board Components

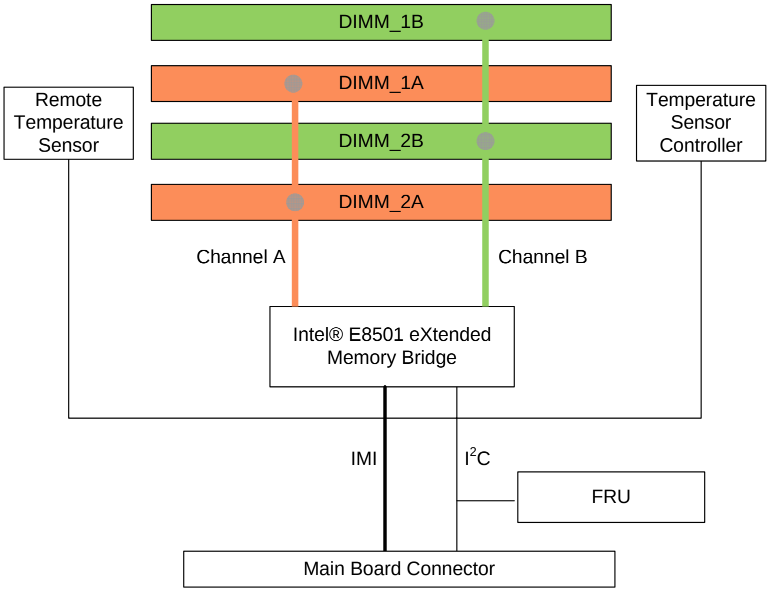

DIMM_1B
DIMM_1A
DIMM_2B
DIMM_2A
Remote Temperature Sensor
Temperature Sensor Controller
Channel A
Channel B
Intel® E8501 eXtended Memory Bridge
IMI
I2C
FRU
Main Board Connector

Figure 6. Memory Board Block Diagram

4.5.1 Button, Retention Latch and LEDs

The following sections provide an overview of the hardware required to support memory hot-plug. See Section 10.1 for more information about memory hot-plug support on the Intel® Server Board Set SE8501HW4.

4.5.1.1 Attention Button

This is a user accessible push button that initiates the proper shut down of the Intel® Server Board Set SE8501HW4 memory board during a memory hot-plug event. When pushed, a notification is sent to the memory hot-plug controller on the mainboard. The system blinks the attention LED until the request can be serviced. The BIOS interprets the request as a hot removal if the memory board is included in the current system memory configuration or as a hot add if it is not.

If the system rejects the removal request, the power LED remains lit. A removal request may be rejected if the current memory mode does not support hot removal. For example if only three good boards in a memory RAID mode remain, the system rejects a removal request to any of those three memory boards. If the system accepts the removal request it blinks the power LED, de-initializes the memory board, then turns off the power LED. After the power LED is turned off, the user may open the retention latch to remove the memory board.

4.5.1.2 Retention Latch

The retention latch is a mechanical lock and handle used to remove the memory board from a chassis and the mainboard. In the event of an unexpected memory hot-plug operation, non-accessible buttons under the retention latch turn off power to the memory board. This safety feature is included to protect the user and circuits in the event that the attention button was not used properly

4.5.1.3 LEDs

All LEDs are controlled by the BIOS through the Independent Memory Interface (IMI). Table 9 describes the LEDs on the Intel® Server Board Set SE8501HW4 memory board.

Table 9. Memory Board LEDs

Name	Color	Description
Mirror	Green	Memory board is in a mirror mode
RAID	Green	Memory board is in a RAID mode
Attention	Amber	When flashing, the memory board is in a hot-plug event
Power[1]	Green	Memory board is powered on, all rails are on
1B	Amber	DIMM_1B has had an error and needs to be replaced
1A	Amber	DIMM_1A has had an error and needs to be replaced
2B	Amber	DIMM_2B has had an error and needs to be replaced
2A	Amber	DIMM_2A has had an error and needs to be replaced

1- The power LED provides indication of the Intel® Server Board Set SE8501HW4 memory board state. It is cleared when the memory board is inactive and set when the memory board is included in the current memory configuration. It blinks when a request is being serviced during a hot removal or hot add event.

4.5.2 Temperature Sensors and FRU

A dual temperature-sensing device provides a sensor at the left and right of the DIMM sockets. Server management sees this as one sensor, measuring the temperature drop across the board, which estimates the heat generated by the DIMMs.

An EEPROM device provides 256 bytes of programmable Field-Replaceable Unit (FRU) space. Like all Intel server boards, this FRU is programmed during manufacturing to contain the board version and serial number but may be programmed to meet integrator-specific needs.

4.5.3 I^{2}C

The XMB, temperature sensor controller, and FRU device are connected to the mainboard Baseboard Management Controller. The I^{2}C bus addressing for these devices is slot dependant and located on private I^{2}C bus 3.

4.5.4 Independent Memory Interface (IMI)

The Independent Memory Interface (IMI) is simultaneous and bi-directional, with a read bandwidth of up to 6.4 GB/s and a write bandwidth of up to 3.2 GB/s. The IMI also provides support for memory board hot-plug signals and protects all transfers with a combination of packet-based CRC and/or x8 SDDC.

4.5.5 Serial Presence Detect (SPD)

The Serial Presence Detect (SPD) bus is a low frequency serial chain that is routed to each DDR2 memory channel. The XMB acts as a master for the SPD bus and uses it to detect and configure the DIMMs.

4.5.6 Power

The mainboard supplies 12V and 3.3V power to the memory board. The memory board has on board regulators to generate 1.8V, 1.5V and 0.9V. The XMB requires 1.5V and 1.8V, the DIMMs require 1.8V and DIMM termination requires 0.9V. The I^{2}C devices use the 3.3V$_{stby}$ from the mainboard.

4.6 Memory Hot-Plug

4.6.1 Prerequisite for Memory Hot-Plug

Before performing a memory board hot remove or add, ensure the system BIOS is configured to support this operation, and the operating system supports this capability. See Section 10.1 for more information about memory modes and their support for memory hot-plug operations.

4.6.2 Memory Board Hot Remove

If the board is already powered on, the following steps are required to ensure proper removal:

10. Press the attention button. The attention LED begins flashing to indicate that the BIOS is preparing the board for a hot remove. The system BIOS copies the data off the board and the attention LED continues to flash as this operation completes.
11. When the attention LED stops flashing and turns off and the power LED has turned off, disengage the retention latch, and remove the memory board. If the power LED does not turn off, the memory configuration may not support memory hot-plug events, see Section 10.1 for more information.

4.6.3 Memory Board Hot Add

1. Plug the memory board into the mainboard and engage the retention latch.
2. Press the attention button to alert the BIOS that a memory board has been added to the system. The BIOS prepares the board for operation and depending on the memory mode, may blink the power LED to indicate the board is not yet available. When the power LED is on the board is in use. If the power LED does not stay solid green, the BIOS has rejected the memory board, see Section 10.1 for more information.

4.7 Memory Board Interoperability

For best performance, the Intel® Server Board Set SE8501HW4 memory board is the preferred memory board for use with the Intel® Server Board Set SE8501HW4 mainboard. The top label indicates 667/800. However, the mainboard is able to operate with the older Intel® Server Board Set SE8500HW4 memory board. Operating the older board affects the FSB speed of the system in accordance with Table 10. Memory Board Interoperability.

Logic has been added to the Intel® Server Board Set SE8501HW4 mainboard that automatically sets the clock frequencies of the processors, NB, and memory boards depending on the speed capability of the inserted processors and memory boards. This speed select logic checks for a frequency match between the inserted processors and memory cards. Memory board speed capability and insertion status is also used to set the speed select logic. The Intel® Server Board Set SE8501HW4 memory board adds a single pin that is used to indicate whether the inserted board is a Intel® Server Board Set SE8501HW4 memory board or the 667 MTS only Intel® Server Board Set SE8500HW4 memory board.

Table 10. Memory Board Interoperability

Board Set	Intel® Server Board Set SE8500HW4 Memory Board	Intel® Server Board Set SE8501HW4 Memory Board
Intel® Server Board Set SE8500HW4 mainboard	667 MTS FSB	667 MTS FSB
Intel® Server Board Set SE8501HW4 mainboard	667 MTS FSB	800 MTS FSB[1]

1. Assumes all installed processors support 800MTS FSB speed.

5. Server Management

Intel® Server Management consists of many embedded technologies that consist of a combination of board instrumentation, sensors, interconnects, server management controllers, firmware algorithms, and the system BIOS. The Intel® Server Management 8.x application provides a systems management application for monitoring server hardware and operating system performance and health. The Intel® Server Deployment Toolkit provides utilities that help integrate server building blocks for optimal operation. This toolkit includes tools for configuring FRU, SDR, firmware, and BIOS; viewing the SEL; and capturing personality (settings) of one server and transferring the personality to another identical server.

The Intel® Server Board Set SE8501HW4 platform management system is based on the *IPMI v2.0 Specification* and includes the following major elements:

- Baseboard Management Controller (BMC) with RTC access
- IPMI messaging, commands, and abstractions
- Sensors for status, voltage, temperature and fan speed
- Sensor Data Records (SDRs) and SDR repository
- Field Replaceable Unit (FRU) information and System Globally Unique ID (GUID)
- Autonomous event logging
- System Event Log (SEL) [3276 events]
- BMC watchdog timer, covering the BIOS and run-time software
- IPMI channels, sessions, and users
- EMP (Emergency Management Port): IPMI messaging over serial/modem. This feature is also referred to as Direct Platform Control (DPC) over serial/modem.
- Serial/modem paging
- Serial/modem/LAN alerting using the Platform Event Trap (PET) format
- DPC (Direct Platform Control): IPMI messaging over LAN (available via onboard network controllers)
- Platform Event Filtering (PEF)
- ICMB (Intelligent Chassis Management Bus) - IPMI messaging between chassis
- IPMI Terminal Mode support
- PCI SMBus support
- Fault Resilient Booting (FRB)
- Magic Packet* and Wake On LAN (WOL) / Power On LAN support
- BIOS logging of POST progress and POST errors
- Integration with the BIOS console redirection via IPMI v1.5 serial port sharing
- Serial Over LAN (SOL) support
- Wake On Ring (WOR) support

Figure 7 shows a logical block diagram of the server management for the Intel® Server Board Set SE8501HW4 and both the Intel Server Platform SR4850HW4/M and Intel® Server Platform SR6850HW4/M.

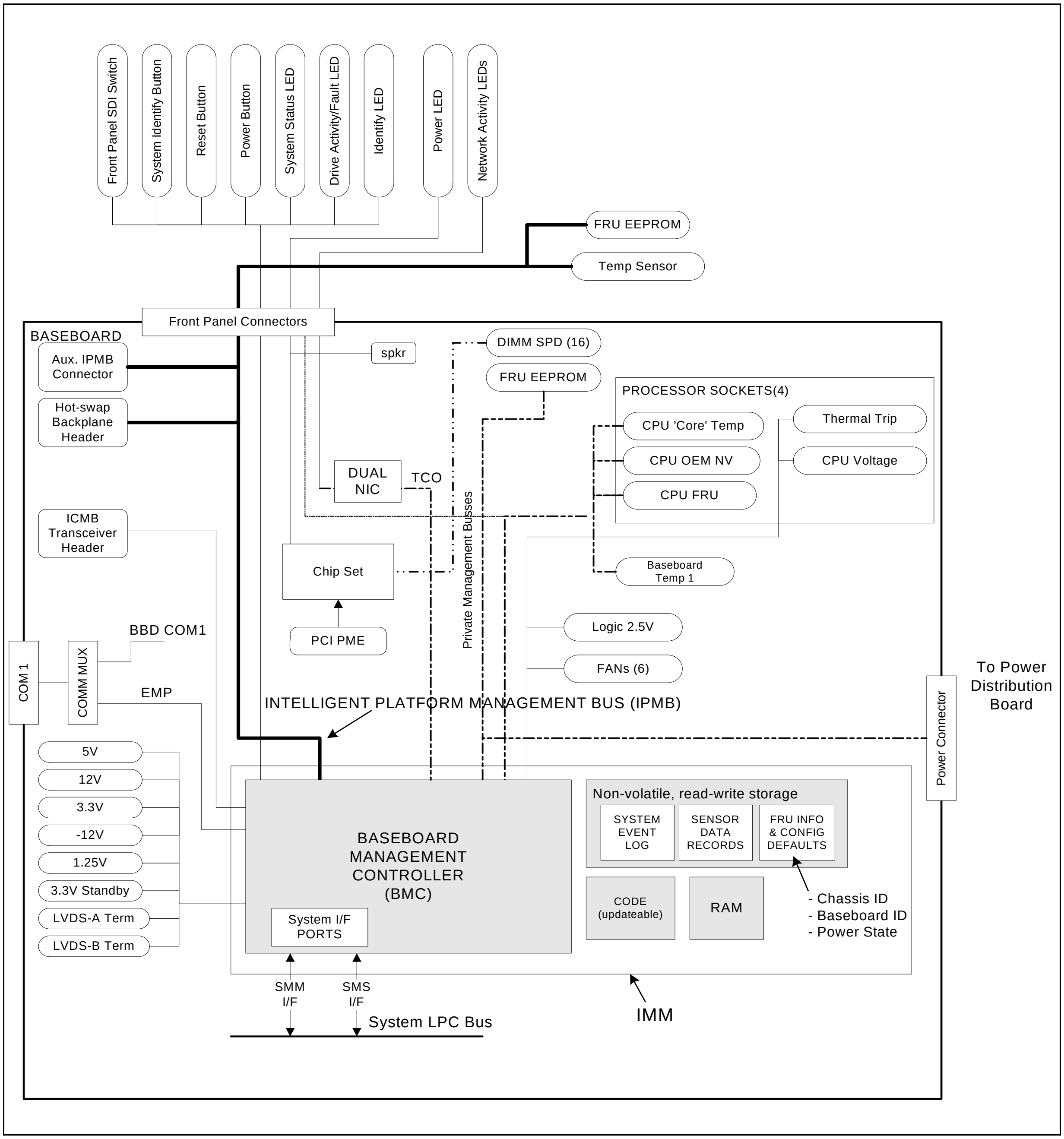


Figure 7. Server Management Block Diagram

Note: The interconnections and blocks shown are to illustrate the functional relationships between the system management elements. They do not map directly to the exact circuit implementation of the architecture.

5.1 Sahalee Baseboard Management Controller (BMC)

The Sahalee Baseboard Management Controller (BMC) contains a 32-bit RISC processor and associated peripherals used to monitor the system for critical events. The Sahalee BMC is designed to be the central server management controller in an enterprise server system. It is common to several Intel® Xeon® processor-based and Intel Itanium® processor-based platform implementations. The Sahalee BMC contains the logic needed for executing the firmware, controlling the system, monitoring sensors, and communicating with other systems and devices via various external interfaces.

The Sahalee BMC resides on an Intel® Management Module that mounts onto the Intel® Server Board Set SE8501HW4 mainboard. Either an Intel® Management Module - Professional Edition or Intel® Management Module - Advanced Edition is required to boot and use the Intel® Server Board Set SE8501HW4. See the *Intel® Management Module Installation and User's Guide* for a description of these parts.

Figure 8 shows the I^{2}C block diagram for Intel® Server Board Set SE8501HW4 and both the Intel® Intel Server Platform SR4850HW4/M and Intel® Server Platform SR6850HW4/M.

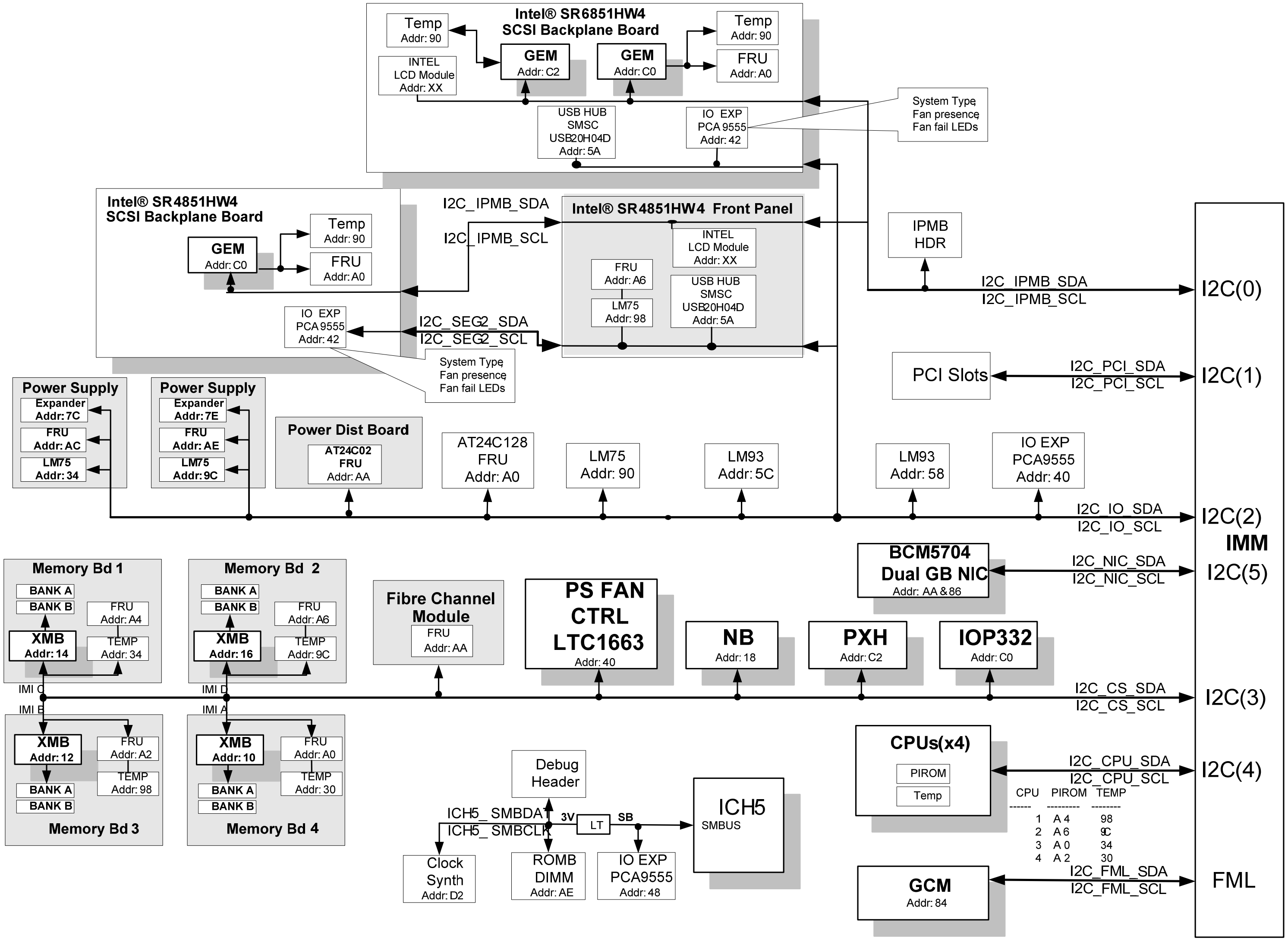


Figure 8. I^{2}C Block Diagram

5.1.1 Sensor Data Record SDR (SDR) Repository

The BMC implements a logical Sensor Data Record (SDR) repository device, as specified in the *Intelligent Platform Management Interface Specification, Version 2.0.* The SDR repository is accessible via all communication transports, even while the system is powered off.

5.1.2 Field Replaceable Unit (FRU) Inventory Devices

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

The BMC provides FRU command access to its own FRU device, as well as to the FRU devices throughout the system. The FRU device ID mappings are shown in Figure 8 and Table 11. The BMC controls the mapping of the FRU device ID to the physical device. Per the IPMI specification, FRU device 0 is always located on the mainboard. By convention, the Intel® Management Module board FRU is always FRU device 1. All Intel-designed server boards maintain onboard non-volatile storage to hold the FRU data.

Table 11. FRU Device Location and Size

FRU Device ID	I^{2}C Bus	I^{2}C Addr	Device	Read Only	Size (bytes)
0	2	0xA0	Mainboard		256
1	2	0xA8	Intel® Management Module		256
2	4	0xA4	Processor 1	Yes	128
3	4	0xA6	Processor 2	Yes	128
4	4	0xA0	Processor 3	Yes	128
5	4	0xA2	Processor 4	Yes	128
6	4	0xA4	Processor 1 OEM		128
7	4	0xA6	Processor 2 OEM		128
8	4	0xA0	Processor 3 OEM		128
9	4	0xA2	Processor 4 OEM		128
10	2	0xA0	LAN		128
11	2	0xA6	Front panel board		256
12	3	0xAA	Power distribution board		256
13	3	0xAC	Power Supply Unit 1	Yes	256
14	3	0xAE	Power Supply Unit 2	Yes	256
15	5	0xAA	Intel® Fibre Channel Module	Yes	256
16	3	0xA0	Memory board A		256
17	3	0xA2	Memory board B		256
18	3	0xA4	Memory board C		256
19	3	0xA6	Memory board D		256

5.1.3 System Event Log (SEL)

The BMC allocates 65,536 bytes of non-volatile space for storing system events. Each event record is padded with an additional four bytes of timestamp, resulting in 20 bytes of storage space per record. A total of 3,276 SEL records can be stored in the system. When an attempt is made to add a SEL record after 3,276 records, the BMC fails the request, an out of space completion code is returned, and the new event is not added to the SEL. The SEL can be cleared in the system BIOS setup, or by using the SEL viewer utility or Intel® Server Management application.

5.1.4 Real-Time Clock (RTC) Access

The chipset on this platform allows the BMC to access the system RTC. This allows the BMC to automatically synchronize the SEL/SDR timestamp clock to the RTC time on BMC startup. This relieves the BIOS from being involved in timestamp management.

5.1.5 Rolling BIOS

The Intel® Server Board Set SE8501HW4 mainboard provides two firmware hubs that can contain two independent BIOS versions. This allows BIOS updates without a system reboot as well as failover to a good BIOS image in the event of BIOS corruption. BMC support for this feature includes the following:

- Persistent storage of the currently selected the BIOS image (firmware hub) and the validity of each image, on the Intel® Management Module
- OEM command support for the BIOS to query/change the currently selected the BIOS image (firmware hub)
- Physical control of the currently selected the BIOS image (firmware hub)

5.1.6 First Boot with a New Intel® Management Module

Since the Intel® Management Module is shared among several Intel server products, a new Intel® Management Module may not be initially programmed with the Intel® Server Board Set SE8501HW4 SDRs and BMC code. After installing a new Intel® Management Module, the user is required to load the Intel® Server Board Set SE8501HW4-specific BMC firmware, SDRs and the BIOS during the first system boot.

The Intel® Management Module contains a persistent flag indicating the firmware hub that contains the primary the BIOS image. During a BIOS update, the new BIOS image overwrites the inactive (secondary) firmware hub. The Intel® Management Module flag is updated to reference the inactive firmware hub as the primary BIOS image and after a reboot, the updated BIOS image loads.

A new Intel® Management Module is programmed to boot using the BIOS image on firmware hub 0. For this reason, users should always update BMC, SDRs, and the BIOS when first installing a module. See Table 12 for an example of rolling BIOS behavior with a new Intel® Management Module.

Table 12. Example Rolling BIOS Behavior with a New Intel® Management Module

Events	Newest BIOS (Available from http://www.intel.com/support/)	Firmware Hub 0	Firmware Hub 1
Server received	BIOS P02	BIOS P01	BIOS P01
New Intel® Management Module installed	BIOS P02	**BIOS P01 (primary)**	BIOS P01 (secondary)
BMC, SDRs, and BIOS updated due to new Intel® Management Module installation	BIOS P02	BIOS P01 (secondary)	**BIOS P02 (primary)**
Server is in use for months	BIOS P03	BIOS P01 (secondary)	**BIOS P02 (primary)**
BIOS updated because a new version is available	BIOS P03	**BIOS P03 (primary)**	BIOS P02 (secondary)
Server is in use for months	BIOS P04	**BIOS P03 (primary)**	BIOS P02 (secondary)
BIOS updated because a new version is available	BIOS P04	BIOS P03 (secondary)	**BIOS P04 (primary)**
Server is in use for months	BIOS P05	BIOS P03 (secondary)	**BIOS P04 (primary)**
New Intel® Management Module installed	BIOS P05	**BIOS P03 (primary)**	BIOS P04 (secondary)
BMC, SDRs, and BIOS updated due to new Intel® Management Module installation	BIOS P05	BIOS P03 (secondary)	**BIOS P05 (primary)**

1. **Bold** indicates primary.

Early in POST, the BIOS communicates a unique platform ID to the BMC and the BMC confirms that the firmware installed matches the indicated platform type. If a platform mismatch occurs, the BMC logs an error to the SEL and configures the system fans to a predefined speed. Near the end of POST, the BIOS again checks for a platform mismatch and displays a warning message on the video. To clear this error, new BMC firmware, SDRs and the BIOS should be loaded.

5.2 Fan Control and Temperature Monitoring

The BMC monitors and controls system fans, with each fan having a tachometer sensor used to determine cooling system health. The fan subsystem has three states: sleep, nominal and boost. Nominal is the default state. In this state fan speeds are based on the ambient system temperature. A system temperature threshold is set via an SDR. When the threshold is exceeded, it linearly ramps the fan speeds either until the fan speed reaches maximum saturation or the temperature reduces below the threshold. If the system temperature stays below the threshold, fan speed ramps back to the default speed. If system temperature remains above the threshold, the system may throttle memory to reduce heat dissipation. Fans are in the sleep state when no fan boost conditions exist and the system is in ACPI S1 sleep state. Table 13 describes when system fans enter the boost state.

Table 13. Fan States

Condition	System Fans	Memory Throttle
Normal power and fan conditions	Vary based on ambient system temperature	No
System intrusion sensor engaged	All high speed (boost)	Yes
System fan failure or removal	All high speed (boost)	Yes
Power supply unit fan failure or removal	All high speed (boost)	No
Platform requires two power supplies, both are installed, but only one AC power cord is connected	All high speed (boost)	No
Power supply failure	All high speed (boost)	No

Note: If there are multiple fan failures, the most recent failure takes precedence.

Fan settings are configurable via SDRs to allow for the specific cooling requirements needed by system integrators. A test command can also be issued to manually force the fan speed to a selected value, overriding any other control or policy.

Ambient system temperature is determined from address 0x90 on private I^{2}C bus 0, which for the Intel Server Platform SR4850HW4/M and Intel Server Platform SR6850HW4/M is a sensor on the SCSI backplane board. The temperature value used by server management is this sensor reading minus 3°C. This sensor address is hard-coded in the BMC and not configured via an SDR value.

5.2.1 Memory Throttling

Memory throttling is the ability of the chipset to reduce bandwidth of the DIMMs when their generated heat exceeds the normal thermal threshold. Each memory board has a temperature-sensing device that provides the difference between the left and right sides of the DIMMs. This difference estimates the heat generated by the DIMMs and is continuously monitored by the BMC. Depending on memory board temperature readings, memory may be throttled back and fans nearby to the memory board(s) may be boosted. Whenever this temperature reaches the upper critical threshold, the BMC requests the XMB on the memory board to enable DIMM throttling. Memory throttling is also enabled when the system intrusion sensor is engaged and in the event of a system fan failure or removal.

5.2.2 Processor Throttling

Processor throttling is the ability of the processor to reduce core speed, and thereby its heat, when generated heat exceeds normal thermal thresholds. The processor can throttle itself, and under the following conditions, the Intel® Server Board Set SE8501HW4 requests a processor to throttle:

- A processor voltage regulator (onboard or module) asserts a thermal trip
- The power consumption threshold of the system is crossed
- BMC requests all processors to throttle

In the Intel® Server Board Set SE8501HW4 the BIOS forces all processors into a throttled condition when any one processor enters this state. Processor throttling is reset after a system reboot.

5.3 ACPI Power Control

The Intel® Server Board Set SE8501HW4 supports ACPI S0, S1 and S5 system/sleep states. The S0 system state is the normal power on state and required for normal system operation. The S1 sleep state is a stand-by power state where part of the systems subsystems are in a powered down or a degraded power state to conserve power when the system is not actively in use. The S5 system state is the normal power off state and is required in order to perform certain maintenance tasks. When the system is operating in ACPI mode, the operating system retains control of the power of the system. During ACPI mode, operating system policy determines the entry methods and wakeup sources for each system/sleep state. An ACPI-enabled operating system generates a System Management Interrupt (SMI) to request that the system enables ACPI support. The BIOS responds to the SMI by communicating to the BMC that ACPI support is required.

5.3.1 S1 Sleep State Support

During this state, the following events take place:

- The front panel power LED blinks at a rate of 1 Hz with a 50% duty cycle.
- The front panel reset button is protected by the BMC to prevent accidental system resets while in this mode.
- If enabled via the set ACPI configuration mode command, the system fans are set to sleep speed.
- The watchdog timer is stopped.

The BMC detects that the system has exited the ACPI S1 sleep state when the S1 sleep signal de-asserted. The BMC passes the state of the front panel power button to the chipset during the S1 sleep state. The chipset then de-asserts the S1 sleep signal when the button is pressed. Sleep state indication ceases whenever the system is powered down (S5).

5.3.2 S5 System State Support

Network adapters hold the wake configuration state for Wake On LAN (WOL). This is typically configured by the operating system and is not cleared by a system reset, though WOL date information should be cleared when going into S5 system state. When a WOL Magic Packet* is received by the BMC, the system powers on if both the following conditions are met:

- WOL is enabled in BIOS setup.
- Chassis intrusion switch is not engaged.

The WOL feature is supported for the onboard, PCI Express* and PCI-X* network adapters.

5.3.3 Secure Mode Operation

The BMC is logically located between the power button and the chipset so that it can implement a secure mode by disabling front panel buttons and add additional power control sources to the system. The BMC passes power control requests to the power button input of the chipset to utilize chipset support for ACPI power control.

Secure mode can be controlled via the Secure Mode KB signal from the keyboard controller. The BMC logs secure mode violation events into the SEL when secure mode is enabled and a user presses front panel buttons that are in a protected state. Secure mode is cleared whenever AC power or system power is applied, when a system reset occurs, or when a BMC reset occurs.

Table 14. Secure Mode Affect on ACPI States

ACPI System State	Power Switch	Reset Switch
S0 (On)	Protected	Protected
S1 (Sleep)	Partial[1]	Protected
S5 (Off)	Unprotected	Unprotected

1. The system wakes from activation of the power switch. Holding the power switch button for four seconds to go to S5 is blocked.

5.4 Fault Resilient Booting (FRB)

When a system reset signal is recognized by the chipset, all processors execute initialization microcode and one is chosen as the bootstrap processor (BSP). The BSP executes the Power On Self Test (POST) for the BIOS and remains the only processor executing commands until control is handed over to an operating system.

Fault Resilient Booting (FRB) is a set of BIOS/BMC algorithms and hardware support that allow, in certain conditions, a multiprocessor system to boot even in the event of a failure with the BSP. The FRB algorithms detect a BSP failure, then disable that processor and reset the system so another processor can be selected as the BSP. For FRB3, the BMC relies on the BIOS to assert the FRB3 timer halt signal, which indicates to the BMC that the BSP is successfully running code.

5.4.1 FRB3

The BMC starts a five-second timer when the system is powered on or hard reset. The BIOS requests the BMC to stop this timer during POST. If the BIOS were able to stop this timer, the BMC assumes that the BSP processor had no errors. If the timer is not stopped and expires, the BMC resets the system. If the timer expires on the second boot, the BMC disables the current BSP, logs the event, selects another BSP, and resets the system.

This process repeats until either the system boots without an FRB3 timeout, or all the processors have been disabled. The BMC enters a desperation mode if all the processors have been disabled. In this mode, the BMC ignores the processor error history and attempt to boot the system one processor at a time. If all the processors have failed in desperation mode, the

BMC enters final desperation mode, where the FRB3 algorithm is disabled and the first processor is allowed to boot into POST. In this mode, a beep code is generated to notify the user the system has reached an FRB3 failure.

FRB3 requires multiple processors. The BMC verifies that there are at least two processors installed in the system. If only one processor is present, the FRB3 timer does not start. The Intel® Server Board Set SE8501HW4 mainboard also includes a jumper to disable the FRB3 timer.

5.4.2 FRB2

The BIOS requests the BMC to start a second 10-minute timer to ensure the system completes the BIOS POST. The FRB2 timer is enabled before the FRB3 timer is disabled to prevent a gap in FRB coverage. The BIOS requests the BMC to disable the FRB2 timer before the option ROMs are scanned, the BIOS setup is entered, or prior to displaying a request for a boot password.

If the FRB2 timer expires and the BIOS is configured with reset as the action to take on the timeout, the BMC logs an FRB2 timeout event with the last POST code generated and reset the system. By default, the BSP processor is not disabled on an FRB2 timeout. There is a BIOS option to disable the processor in an FRB2 timeout, but since this timeout may not be a processor failure, the default behavior is to only reset the system. If during the next boot the BIOS can determine that the last boot failure was processor related, the BIOS requests the BMC to disable the BSP and reset the system.

5.5 Reset Control

Reset circuitry on the Intel® Server Board Set SE8501HW4 mainboard is aware of resets from several sources and determines the proper reset sequence for the different types of resets. Table 15 defines all the reset sources and the actions taken by the system.

Table 15. System Reset Sources and Actions

Reset Source	System Reset?	BMC Reset?
Standby power comes up	No (no DC power)	Yes
Main system power comes up	Yes	No
Reset button pushed	Yes	No
Warm reset	Yes	No
Set processor state or chasis control command	Yes	No
Watchdog timer configured for reset	Yes	No
FRB3 timeout	Yes	No
PEF action	Optional	No
Exit BMC firmware update mode	No	Yes

5.5.1 Front Panel Reset

The reset button is a momentary contact button on the front panel. It is routed through the front panel connector to the BMC, which monitors and de-bounces the signal.

If secure mode is enabled, or the button is forced protected, the reset button does not reset the system, and a platform security violation attempt event message is logged. The reset button is also disabled in sleep mode.

5.5.2 Warm Reset

A warm reset does not remove power from the system and is usually triggered by software or from the ICH5 (e.g. when Ctrl-Alt-Del is pressed). This reset can also result if the BMC detects that the FRB3 timer halt signal has become de-asserted after having previously been asserted by the BIOS to disable the FRB3 timer.

5.6 Remote Management and External Interfaces to the BMC

Several external BMC interfaces are available to enable a variety of options for remote server management. Additional detail on most of these interfaces can be obtained from the *IPMI 2.0 Specification*. Figure 9 provides an overview of the interfaces and the sections that follow describe platform-specific implementation.

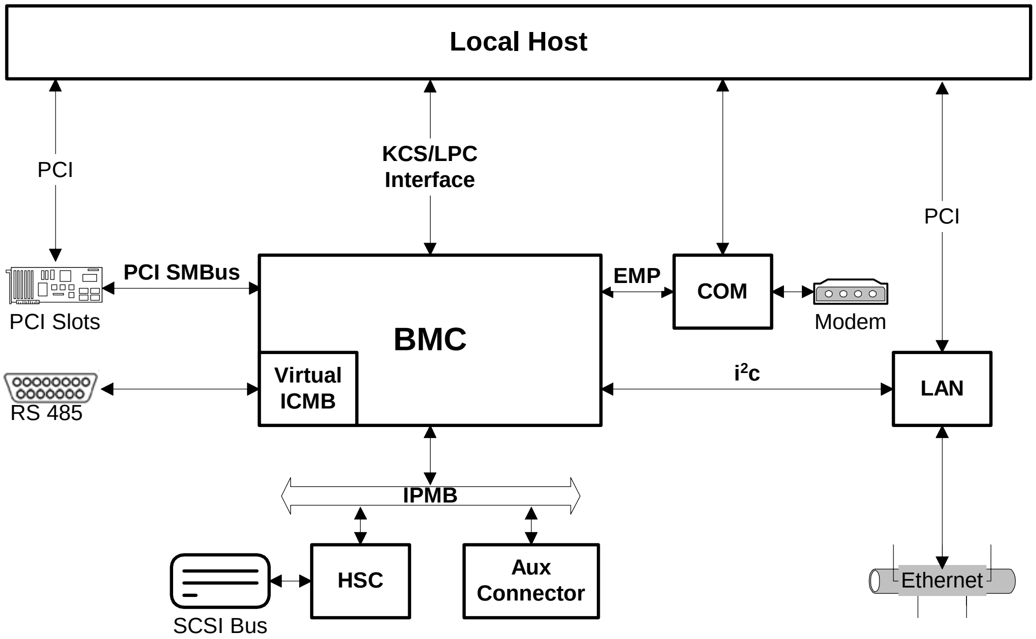


Figure 9. External Interfaces to the BMC

5.6.1 Intelligent Platform Management Buses (IPMB)

The IPMB is a communication protocol that utilizes a 100 KB/s I^{2}C bus. The IPMB implementation in the BMC is compliant with the *IPMB v1.0, revision 1.0*, with the BMC having an IPMB slave address of 0x20.

The BMC both sends and receives IPMB messages over the IPMB interface. Non-IPMB messages received via the IPMB interface are discarded. In addition to the public IPMB, the BMC has six private I^{2}C buses that extend throughout the system. Table 16 shows all the I^{2}C buses in the Intel® Server Board Set SE8501HW4 and Intel® Server Platform SR4850HW4/M and/or SR6850HW4/M, and Figure 8 shows a graphical representation of these buses.

Table 16. Platform I^{2}C Buses

Physical I^{2}C Bus #	Active with Standby Power Only	Private Bus ID	Logical I^{2}C Bus ID	Bus Name	Devices Connected
0	Y	-	0	IPMB	Hot Swap Controllers, IPMB Aux connector, LCD Module
1	Y	-	2	PCI	PCI Bus slots
2	Y	2	5	IO	PCA9555, LM93 (two), LM75, FRU, power distribution board, Power Supply Units (two)
3	N	3	7	CS	XMB (four), FC module, NB, PXH, Intel® IOP332 Storage I/O Processor
4	Y	4	9	Processors	Processors (four)
5	Y	5	B	NIC	On-board networking

5.6.2 Keyboard Controller Style (KCS)/Low Pin Count (LPC) Bus

The BMC has three KCS interface ports as described in the IPMI 2.0 specification. These interfaces are used to communicate SMI handling for error logging, BIOS POST, utility access and power management communication. The BMC also acts as a bridge between the SMS and IPMB interfaces.

5.6.3 Intelligent-Chassis Management Bus (ICMB)

The Intelligent Chassis Management Bus (ICMB) defines a character-level transport for inter-chassis communications between intelligent chassis. This includes the ability to use the ICMB to bridge messages from the IPMB in one chassis to the IPMB in another. At any given time, only one chassis can be driving the bus. Each must arbitrate to gain control of the bus when it has something to send. ICMB messages are IPMI compatible with an implicit net function of bridge. Refer to *Intelligent Chassis Management Bus, Version 1.0, Revision 1.20* for the definition of commands and responses. The Intel® Server Board Set SE8501HW4 provides the ICMB interface as an add-in transceiver card connected to the 5-pin ICMB header.

5.6.4 Serial Over LAN (SOL)

Serial Over LAN (SOL) provides bi-directional transport of system COM2 serial data encapsulated in IPMI over LAN packets. This provides out-of-band LAN access to the BIOS console redirection, service partition application communication, or operating system console interaction without the BIOS or software being LAN-enabled or aware of anything beyond a serial port interface. The console type is set to VT100+ and data bits are set to 8bits/charatecter, no parity and one stop bit as per IPMI messaging requirement.

The BMC supports the Intel proprietary SOL (now known as SOL 1.0) as well as the IPMI 2.0-defined SOL feature, implemented as a standard payload type over RMCP+. The Intel® Server Board Set SE8501HW4 provides the SOL interface via the Generic Communication Module (GCM) port and Intel® Management Module - Advanced Edition.

5.6.5 Emergency Management Port (EMP) Interface

The EMP interface is the Intel implementation of the IPMI 2.0 over serial/modem feature, providing an out-of-band RS232 connection into the server management subsystem. This gives system administrators the ability to access low-level server management firmware functions by using commonly available tools. To make it easy to use and provide the most compatibility with LAN and IPMB protocols, the protocol adopts some features of both protocols.

Both the basic and PPP/UDP proxy modes of IPMI over serial/modem are supported and are available regardless of the system DC power state. The callback feature is also supported to provide another level of server security. Hardware handshaking, Ring Indicate (RI), and Data Carrier Detect (DCD) signals are also supported.

The Intel® Server Board Set SE8501HW4 provides the EMP interface through the COM1 connector. The BMC has control over which agent (BMC or system) has access to COM1.

5.7 Event Filtering and Alerting

The BMC implements the following IPMI 2.0 alerting features:

- Platform Event Filtering (PEF)
- Dial Page Alerting
- Alert over LAN
- Alert over Serial/PPP

5.7.1 Platform Event Filtering (PEF)

The Platform Event Filtering (PEF) feature provides a configurable mechanism to allow SEL events to trigger alert actions. PEF provides a flexible, general mechanism that enables the BMC to perform selectable actions triggered by a configurable set of platform events. The BMC supports the following PEF actions:

- Power Off
- Power Cycle
- Reset
- Diagnostic Interrupt

- OEM Action
- Alerts

Both PEF startup delay disable and alert/non-alert actions after power low are not supported by the BMC.

The Intel® Server Board Set SE8501HW4 supports a maximum of 20 PEF table entries. Table 17 describes the 12 default configured event filters. The remaining eight entries are configurable via software. Each PEF entry contains four bytes of data for a maximum table size of 80 bytes. Associated with each PEF entry is an alert policy that determines whether the alert is a dial page or PPP alert, and over which IPMI channel the alert should to be sent. There is a maximum of 20 alert policy entries, with no pre-configured entries in the alert policy table.

Table 17. Default Event Filters

Event Filter #	Offset Mask	Events
1	Non-critical, Critical & Non-recoverable	Temperature Sensor out of range
2	Non-critical, Critical & Non-recoverable	Voltage Sensor out of range
3	Non-critical, Critical & Non-recoverable	Fan Failure
4	General Chassis Intrusion	Chassis Intrusion [Security Violation]
5	Failure & Predictive Failure	Power Supply Failure
6	Uncorrectable ECC	BIOS (MCA Handler)
7	POST Error	BIOS: Post Code Error
8	FRB2 & FRB3	FRB Failure
9	-	Reserved (no source for Fatal NMI on this platform)
10	Power Down, Power Cycle & Reset	Watchdog Timer
11	OEM System Boot Event	System Restart (Reboot)
12	-	Reserved

5.7.2 Dial Page Alerting

Dial page alerting operates using an external modem connected to the system's onboard EMP serial connection on COM2. With dial paging, the system can be configured to automatically dial up a paging service when a platform event occurs. Dial page alerting is an alert type supported by Platform Event Filtering (PEF). A dial page alert can be initiated by the arrival of an event that triggers the PEF Dial Page action or it can be initiated by an Alert Immediate command with appropriate parameters.

The following dial page resource sizes are platform -specific. Refer to the Intel® Server Platforms SR4850HW4/M and SR6850HW4/M Firmware External Product Specification for their values.

- Alert String Count
- Dial String Count (shared with Alert over Serial/PPP)
- Serial/Modem Alert Destination Count (shared with Alert over Serial/PPP)

Refer to the *IPMI 1.5 Specification* for additional details on this feature.

5.7.3 Alert over LAN

Two types of alerts are supported over LAN.

- Platform Event Trap (PET) alerts – Standard and Advanced
- SMTP Alerts – Advanced (Dedicated NIC only)

The alert over LAN feature is used to notify remote system management application of PEF selected events regardless of the state of the host's operating system. LAN alerts may be sent over any of the LAN channels supported by a platform, modulo the specific channel capabilities. The BMC implements three OEM PEF parameters associated with PET Alerts over LAN.

- PET OEM String (parameter 96), if defined, is included as part of the PET packet OEM data field.
- Infinite Retry Alert Behavior (parameter 97), a byte value where if equal to one, indicates that the Alert over LAN feature should retry Alerts until they succeed.
- UTC Offset (parameter 98), this parameter provides a value for the UTC Offset field in the PET packet.

The following Alert over LAN resource is platform-specific. Refer to the Intel® Server Platforms SR4850HW4/M and SR6850HW4/M Firmware External Product Specification for specific values.

- LAN Alert Destination Count

Refer to *IPMI 2.0 Specification* for additional details on PET Alerts feature.

5.7.4 Alert over Serial/PPP

Alert over Serial/PPP uses the same IP/UDP packet encapsulation as Alert over LAN, but allows alerts to be delivered via modem to a PPP enabled destination. An alert can trigger a dial out to one or more destinations as specified in the Alert Policy table, Serial/Modem Destination, and PPP Account parameters.

The following Alert over Serial/PPP resource sizes are platform-specific. Refer to the platform BMC Technical Product Specification for their values.

- Alert String Count
- Alert String Size
- Dial String Count (shared with Dial Page Alerting)
- Serial/Modem Alert Destination Count (shared with Dial Page Alerting)
- Serial/Modem Destination IP Address Count
- PPP Account Count

Microsoft CBCP* (Callback Control Protocol) is not supported.

Refer to *IPMI 2.0 Specification* for additional details on this feature.

6. Jumpers

6.1 Mainboard

Please refer to the jumper descriptions below in Table 18. Mainboard Jumpers.

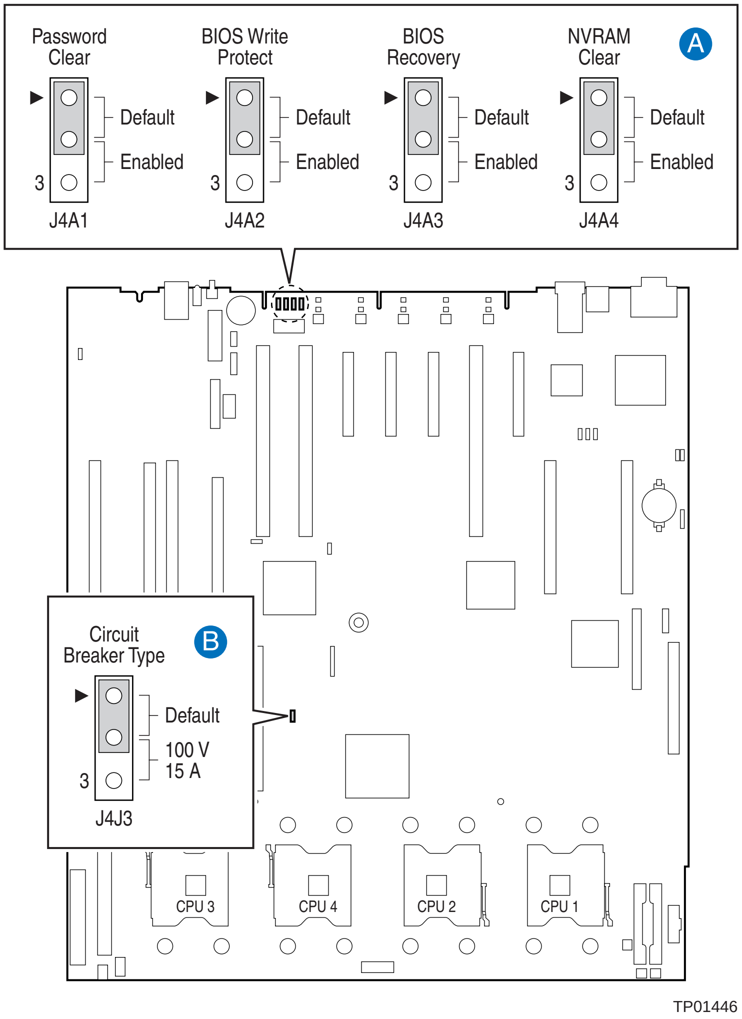


Figure 10. Mainboard Jumper Locations

Table 18. Mainboard Jumpers

Name	Location	Default	Stuffed Jumper State (Default in Bold)
Password Disable or Clear	J4A1	Stuff Empty	1 – 2 = Password Enabled 2 – 3 = Password Disabled / Cleared
BIOS WP	J4A2	Stuff Empty	1 – 2 = BIOS Unprotected 2 – 3 = BIOS write protected
BIOS Recovery	J4A3	Stuff Empty	1 – 2 = Normal Boot 2 – 3 = BIOS Recovery
BIOS Clear CMOS/NVRAM	J4A4	Stuff Empty	1 – 2 = BIOS_CLR_CMOS 2 – 3 = Forced CMOS/NVRAM clear
CB_TYPE (circuit breaker type)	J4G3	Stuff Empty	1 – 2 = Circuit Breaker – Other 2 – 3 = Circuit Breaker – 100V 15Amp
PHPDIS (PCI Hot-Plug diable)	J4G5	Stuff Empty	1 – 2 = PHP Enabled 2 – 3 = PHP Disabled
FRB3 Disable	J8C1	Stuff Empty	1 – 2 = FRB3 timer enabled 2 – 3 = FRB3 timer disabled
BMC RESET	J8C2	Stuff Empty	1 – 2 = BMC enabled 2 – 3 = BMC Disabled
FWHID	J8C3	Stuff Empty	1 – 2 = Enables BMC controls FWHID swap 2 – 3 = Force FWHID swap

6.1.1 Circuit Breaker Type Jumper

Jumper J4G3, shown by letter “B” in Figure 10, is used to set a threshold for power consumption when operating the server with a single power supply on a lot-line 100/110/115/120/127VAC power circuit. This threshold is required to ensure the power consumption of the server does not exceed the power that can be supplied by a single AC power circuit. When the system has two power supplies installed, a separate AC power circuit is needed for each power supply to guarantee the AC power circuit capability is not exceeded.

When a server is connected to low-line power, the J4G3 jumper sets the following power consumption thresholds:

- Pins 1-2 covered: Sets the power consumption threshold to 1350 watts
- Pins 2-3 covered: Sets the power consumption threshold to 1100 watts

Power consumption is based on the power consumed within the system. Power factors for inefficiency are not included in the above figures.

Servers connected to high-line power (200/208/220/230/240VAC) do not have a power consumption threshold. Under these conditions, the J4G3 jumper should be set as follows:

- 100/110VAC rated circuit: Cover pins 2-3
- 115/120/127VAC rated circuit: Cover pins 1-2
- 200/208/220/230/240VAC rated circuit: Cover pins 1-2

The power consumption threshold is most likely to be exceeded when all of the following conditions are met:

- The server is connected to a low-line power circuit
- The server has a single power supply installed
- The server is fully configured with four processors, 16 x4 GB DIMMs, and all PCI slots are filled
- The server is running at maximum performance

If the power consumption threshold is crossed, the hardware throttles the processors to reduce the power consumption to below the set threshold. The processor performance can be returned to the full performance level by power cycling the server.

When two power supplies are installed, the required power is divided between them. By using both circuits, the server can draw more power than the threshold limit for a single power supply. The hardware reduces the amount of power consumed if one of the power supplies fails. This ensures the system consumes less power than the threshold from the single operating power supply. When a failed power supply is replaced, the system is again able to share the power load and operate at full performance.

If the J4G3 jumper is set incorrectly, the following may occur:

- If the jumper is covering pins 1-2 on a 100/110VAC circuit, the server is allowed to consume up to 1350 watts. This setting may cause a circuit breaker to trip.
- If the jumper is covering pins 2-3 on a 115/120/127VAC circuit, the server power consumption threshold is set to 1100 watts. The lower power threshold may be exceeded, limiting system performance.

6.1.2 Intel® Management Module

The BMC boot block area of the Intel® Management Module flash device is physically protected by a jumper. This jumper must be changed in order to enable updating the boot block. The BMC firmware transfer code does sense the state of this jumper and always allow writes to the boot block area. If the jumper is not in the enabled position, the boot block writes fail. Please refer to BMC release notes and the *Intel® Management Module Technical Product Specification* for more information.

7. Connectors

7.1 SCSI

The Intel® Server Board Set SE8501HW4 mainboard has two unshielded 68-pin SCSI connectors for SCSI channel A and B.

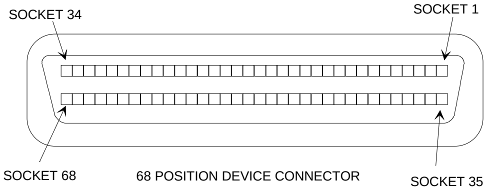


Figure 11. 68-Pin SCSI Connector

Table 19. 68-Pin SCSI Connector Pinout

Pin	Signal	Pin	Signal
1	SCSI(A:B)_DB_P12	35	SCSI(A:B)_DB_N12
2	SCSI(A:B)_DB_P13	36	SCSI(A:B)_DB_N13
3	SCSI(A:B)_DB_P14	37	SCSI(A:B)_DB_N14
4	SCSI(A:B)_DB_P15	38	SCSI(A:B)_DB_N15
5	SCSI(A:B)_DB_PP1	39	SCSI(A:B)_DB_NP1
6	SCSI(A:B)_DB_P0	40	SCSI(A:B)_DB_N0
7	SCSI(A:B)_DB_P1	41	SCSI(A:B)_DB_N1
8	SCSI(A:B)_DB_P2	42	SCSI(A:B)_DB_N2
9	SCSI(A:B)_DB_P3	43	SCSI(A:B)_DB_N3
10	SCSI(A:B)_DB_P4	44	SCSI(A:B)_DB_N4
11	SCSI(A:B)_DB_P5	45	SCSI(A:B)_DB_N5
12	SCSI(A:B)_DB_P6	46	SCSI(A:B)_DB_N6
13	SCSI(A:B)_DB_P7	47	SCSI(A:B)_DB_N7
14	SCSI(A:B)_DP0_P	48	SCSI(A:B)_DP0_N
15	GND	49	GND
16	SCSI(A:B)_DIFFSENSE	50	GND
17	SCSI(A:B)_TERMPWR	51	SCSI(A:B)_TERMPWR
18	SCSI(A:B)_TERMPWR	52	SCSI(A:B)_TERMPWR
19	RESERVED (NC)	53	RESERVED
20	GND	54	GND
21	SCSI(A:B)_ATN_P	55	SCSI(A:B)_ATN_N
22	GND	56	GND
23	SCSI(A:B)_BSY_P	57	SCSI(A:B)_BSY_N
24	SCSI(A:B)_ACK_P	58	SCSI(A:B)_ACK_N
25	SCSI(A:B)_RST_P	59	SCSI(A:B)_RST_N

Pin	Signal	Pin	Signal
26	SCSI(A:B)_MSG_P	60	SCSI(A:B)_MSG_N
27	SCSI(A:B)_SEL_P	61	SCSI(A:B)_SEL_N
28	SCSI(A:B)_CD_P	62	SCSI(A:B)_CD_N
29	SCSI(A:B)_REQ_P	63	SCSI(A:B)_REQ_N
30	SCSI(A:B)_IO_P	64	SCSI(A:B)_IO_N
31	SCSI(A:B)_DB_P8	65	SCSI(A:B)_DB_N8
32	SCSI(A:B)_DB_P9	66	SCSI(A:B)_DB_N9
33	SCSI(A:B)_DB_P10	67	SCSI(A:B)_DB_N10
34	SCSI(A:B)_DB_P11	68	SCSI(A:B)_DB_N11

7.2 100-pin Front Panel

The Intel® Server Board Set SE8501HW4 mainboard has one 100-pin connector.

Table 20. 100-pin Front Panel Connector Pinout

Pins	Signals
1,3,7,10,14,20,27,42,51,52,54,58,62,65,73,77,79,82,83,85,87,89,91,93,95,100	Ground
4,6,8,12,13,15,17,19,22,24,26,29,31,33,35,37,41,44,46,48,50,53,56,59,61,66,68,70,72	Unused

Table 21. 100-pin Connector Signal Description

Pin	Signal Name	Signal Description
2	GND – RESISTOR	Ground through zero ohm resistor
5	GND – RESISTOR	Ground through zero ohm resistor
9	GND – RESISTOR	Ground through zero ohm resistor
11	GND – RESISTOR	Ground through zero ohm resistor
16	FAN1_TACH	Fan 1 Tachometer signal – edges per revolution
18	FAN2_TACH	Fan 2 Tachometer signal – edges per revolution
21	FAN3_TACH	Fan 3 Tachometer signal – edges per revolution
23	FAN4_TACH	Fan 4 Tachometer signal – edges per revolution
25	RESET_BTN	Front panel reset button signal
28	FAN5_TACH	Fan 5 Tachometer signal – edges per revolution
30	FAN6_TACH	Fan 6 Tachometer signal – edges per revolution
32	FAN_PWM1	Zone 1 Fan PWM control signal
34	5VSTANDBY	5Vstandby to front panel
36	BP_D2D_EN	Backplane D2D enable
38	5VSTANDBY	5Vstandby to front panel
39	ICH5_PDD8	IDE primary disk data 8
40	HD_ACT_N	SATA Hard Drive Activity
43	BP_PWRGOOD	Back Plane power good signal
45	PCI_RST_BP_N	PCI reset to backplane

Pin	Signal Name	Signal Description
47	CP_PWR_LED	Control Panel Power LED signal
49	CP_SPKR_OUT_N	Speaker signal to front panel
55	NIC1_LED	NIC 1 activity LED signal
57	ID_LED	ID LED Signal
60	CP_BTN_PWR_ON	Control panel Power Button signal
63	SYS_STATUS_AMB_LED	System Status amber LED signal
64	CD_PRES_N	CD drive presence signal
67	CP_ID_BUTTON_RAW	Control panel ID button signal
69	CP_BTN_NMI	Control panel NMI button
71	NIC2_LED	NIC2 activity LED signal
74	I2C_IPMB_SCL	IPMB I2C bus clock
75	BP_PRES_N	SCSI backplane board presence signal
76	I2C_IPMB_SDA	IPMB I2C bus data
78	SYS_PWRGD4	Mainboard power good signal to SCSI backplane board
80	USB_FRONT_N	USB port 2 differential negative signal to front bezel
81	USB_FRONT_P	USB port 2 differential positive signal to front bezel
84	VID_RED_FRONT	Video DAC 2 RED signal
86	VID_BLUE_FRONT	Video DAC 2 BLUE signal
88	VID_GREEN_FRONT	Video DAC 2 GREEN signal
90	VID_HS_OUT_FRONT	Video DAC 2 horizontal synchronization signal
92	VID_VS_OUT_FRONT	Video DAC 2 vertical synchronization signal
94	VID_DDC_OUT_SCLK_FRONT	Video monitor detection I2C bus clock
96	VID_DDC_OUT_SDA_FRONT	Video monitor detection I2C bus data
97	I2C_CP_SDA	Control panel I2C bus data (I2C segment 2)
98	SYS_STATUS_GRN_LED	System status green LED signal
99	I2C_CP_SCL	Control panel I2C bus data (I2C segment 2)

7.3 COM2 Serial Port

The Intel® Server Board Set SE8501HW4 has one internal serial header that serves as the interface to the COM2 serial port.

Table 22. COM2 Serial Header Pinout

Pin	Signal	Description
1	DCD_N	Data Carrier Detect
2	DSR_N	Data Set Ready
3	RXD	Receive Data
4	RTS_N	Request To Send
5	TXD	Transmit Data
6	CTS_N	Clear To Send
7	DTR_N	Data Terminal Ready
8	RI_N	Ring Indicator
9	GND	GND

7.4 USB

The Intel® Server Board Set SE8501HW4 has one internal USB 2.0 header.

Table 23. 4-pin Internal USB Header

Pin	Signal
1	Fused Voltage Controlled Current (VCC) (+5 V with over-current monitoring)
2	USBP2N (differential data line)
3	USBP2P (differential data line)
4	GND (ground)

7.5 SATA

The Intel® Server Board Set SE8501HW4 has one Serial ATA (SATA) header.

Table 24. SATA Connector Pinout

Pin	Signal
1	Ground
2	A+
3	A-
4	Ground
5	B-
6	B+
7	Ground

7.6 Power

The Intel® Server Board Set SE8501HW4 has three connectors for the power subsystem, two 12-pin connectors that provide primary power and one 2x15 header for power subsystem signals and 3.3V$_{stby.}$

Table 25. 12-pin Power Connector Pinout

Pins	Signal
1-6	GND
7-12	+12V

Table 26. 30-pin Power Signal Header Pinout

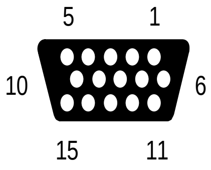
Pins	Signal Description
1,17,25,30	GND
6,7,10,12,14,15,24	$3.3V_{stby}$
2	PS1 present
3	PS2 AC good
4	PS Fan control
5	PS1 AC good
8	PS1 AC range
9	PS on
11	I^2C SCL
13	I^2C SDA
16	12V Sense return
18	PS 90% utilization
19	PS 74% utilization
20	PS 45% utilization
21	PS 37% utilization
22	Int alert
23	PS2 AC range
26	PS1 AC good
27	12V Sense
28	PS1 power OK
29	PS2 present

7.7 Rear Panel Connectors

7.7.1 Video

The Intel® Server Board Set SE8501HW4 has one standard 15-pin video connector.

Table 27. Video Connector Pinout

Pin	Signal Name and Description	Video Connector
1	VID_R (analog color signal red)	
2	VID_G (analog color signal green)	
3	VID_B (analog color signal blue)	
4	No connection	
5	GND	
6	GND	
7	GND	
8	GND	
9	No connection	

Pin	Signal Name and Description	Video Connector
10	GND	
11	No connection	
12	MONID1 (to support DDCx, Display Data Channel* standard)	
13	VID_HSYNC (horizontal sync)	
14	VID_VSYNC (vertical sync)	
15	MONID2 (to support DDCx, Display Data Channel standard)	

7.7.2 Network

The Intel® Server Board Set SE8501HW4 has two stacked RJ45 networking ports with integrated LEDs. LAN1 is on the top, LAN2 on the bottom.

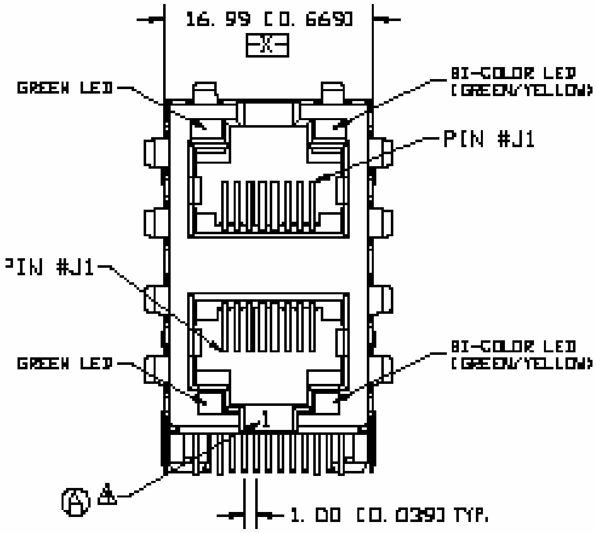


Figure 12. Stacked Ethernet Connector

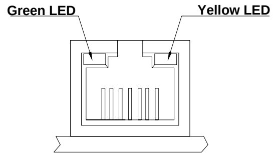
Table 28. Stacked Ethernet Connector Pinout

Pin	Signal	Description
LED Signals		
27	DNW_LINKB10_N	Lower (LAN2) green status LED cathode signal indicating LAN2 activity
28	DNW1_ACT_N_R	Lower (LAN2) green status LED anode to 100-ohm pullup to 3.3V Standby
29	DNW_LINKB100_N	Lower (LAN2) green speed LED cathode, yellow LED anode
30	LANB1000_N_R	Lower (LAN2) yellow speed LED cathode, green LED anode
31	DNW_LINKA10_N	Upper (LAN1) green status LED cathode signal indicating LAN1 activity
32	DNW0_ACT_N_R	Upper (LAN1) green status LED anode to 100-ohm pullup to 3.3V Standby

Pin	Signal	Description
33	DNW_LINKA100_N	Upper (LAN1) green speed LED cathode, yellow LED anode
34	LANA1000_N_R	Upper (LAN1) yellow speed LED cathode, green LED anode
Ethernet Signals		
15	DNW_MDIB_DP<0>	LAN2 transceiver 0 positive of differential pair
21	DNW_MDIB_DN<0>	LAN2 transceiver 0 negative of differential pair
23	DNW_MDIB_DP<1>	LAN2 transceiver 1 positive of differential pair
16	DNW_MDIB_DN<1>	LAN2 transceiver 1 negative of differential pair
18	DNW_MDIB_DP<2>	LAN2 transceiver 2 positive of differential pair
24	DNW_MDIB_DN<2>>	LAN2 transceiver 2 negative of differential pair
26	DNW_MDIB_DP<3>	LAN2 transceiver 3 positive of differential pair
19	DNW_MDIB_DN<3>	LAN2 transceiver 3 negative of differential pair
6	DNW_MDIA_DP<0>	LAN1 transceiver 0 positive of differential pair
13	DNW_MDIA_DN<0>	LAN1 transceiver 0 negative of differential pair
11	DNW_MDIA_DP<1>	LAN1 transceiver 1 positive of differential pair
5	DNW_MDIA_DN<1>	LAN1 transceiver 1 negative of differential pair
3	DNW_MDIA_DP<2>	LAN1 transceiver 2 positive of differential pair
10	DNW_MDIA_DN<2>	LAN1 transceiver 2 negative of differential pair
8	DNW_MDIA_DP<3>	LAN1 transceiver 3 positive of differential pair
2	DNW_MDIA_DN<3>	LAN1 transceiver 3 negative of differential pair
Power Signals		
4, 7, 9, 12, 14, 17, 22, 25	+1.8V Standby	
1, 20, 35, 36, 37, 38	Chassis Ground	Ground

The Intel® Server Board Set SE8501HW4 also provides an RJ45 connector that connects to the Intel® Management Module - Advanced Edition for out-of-band server management features. This out-of-band connector is also referred to as the Generic Communication Module (GCM), or server management Ethernet controller.

Table 29. Server Management Ethernet Connector Pinout

Pins	Signal	Description	Server Management Ethernet Connector
1	GCM_NIC_RDM		
2	GCM_NIC_RDP		
3-6		Magnetics Tap	
7	GCM_NIC_TDM		
8	GCM_NIC_TDP		
A1	TP_GCM_RJ45_YEL_LED_A	Yellow LED Anode	
C1	TP_GCM_RJ45_YEL_LED_C	Yellow LED Cathode	
A2	GCM_NIC_ACTLED_N	Green LED Anode	
C2	GCM_NIC_ACTLED_R_N	Green LED Cathode	

7.7.3 COM1 Serial Port

The Intel® Server Board Set SE8501HW4 has one DB9 port that can be either COM1 or the Emergency Management Port for remote server management.

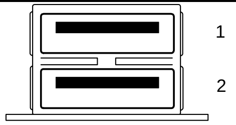
Table 30. COM1 Serial Port Pinout

Pin	Signal	Description
1	DCD_N	Data Carrier Detect
2	RXD	Receive Data
3	TXD	Transmit Data
4	DTR_N	Data Terminal Ready
5	GND	GND
6	DSR_N	Data Set Ready
7	RTS_N	Request To Send
8	CTS_N	Clear To Send
9	RI_N	Ring Indicator

7.7.4 USB

The Intel® Server Board Set SE8501HW4 has one stacked USB 2.0 connector.

Table 31. Stacked USB Connector Pinout

Pin	Signal	USB Connector
A1	Fused Voltage Controlled Current (VCC) (+5 V with over-current monitoring)	 **Dual Stacked USB Connector**
A2	USBPxN (differential data line)	
A3	USBPxP (differential data line)	
A4	GND (ground)	
B1	Fused VCC (+5 V with over-current monitoring)	
B2	USBPxN (differential data line)	
B3	USBPxP (differential data line)	
B4	GND (ground)	

7.8 Server Management and Diagnostics

7.8.1 5-pin ICMB Header

Table 32. 5-pin ICMB Header Pinout

Pin	Signal
1	$5V_{stby}$
2	ICMB Tx
3	ICMB Tx EN
4	ICMB Rx
5	GND

7.8.2 3-pin IPMB Header

Table 33. 3-pin IPMB Header Pinout

Pin	Signal
1	IPMB SDA
2	GND
3	IPMB SCL

7.8.3 3-pin Chassis Intrusion

Table 34. 3-pin Chassis Intrusion Pinout

Pin	Signal
1	Intrusion event
2	GND
3	Intrusion button attached

7.8.4 I^{2}C POST Code Headers

The Intel® Server Board Set SE8501HW4 mainboard has a 5-pin header (with the fourth pin removed) for an I^{2}C POST-code card. The I^{2}C signals are from the SMB bus in the ICH5. The data and clock signals are pulled up to 3.3V$_{stby}$.

Table 35. 5-pin I^{2}C POST Code Header Pinout

Pin	Signal
1	12 V Standby
2	SMBDATA
3	SMBCLK
4	NC – pin removed
5	Ground

8. Electrical Specifications

8.1 Power Generartion

Input power to the Intel® Server Board Set SE8501HW4 mainboard is 12V and $3.3V_{stby}$. All other required voltages are generated by Voltage Regulator Down (VRD) circuits and Voltage Regulator Modules (VRMs) on the mainboard. The processor core voltages for processor sockets 1 and 2 are generated by VRDs and processors 3 and 4 get their core voltage from VRMs. One VRD generates the cache voltage for processors 1 and 2, and an L3 cache VRM9DO provides cache voltage for processors 3 and 4, when those sockets are used by 64-bit Intel® Xeon® Processors MP with up to 8MB L3 cache.

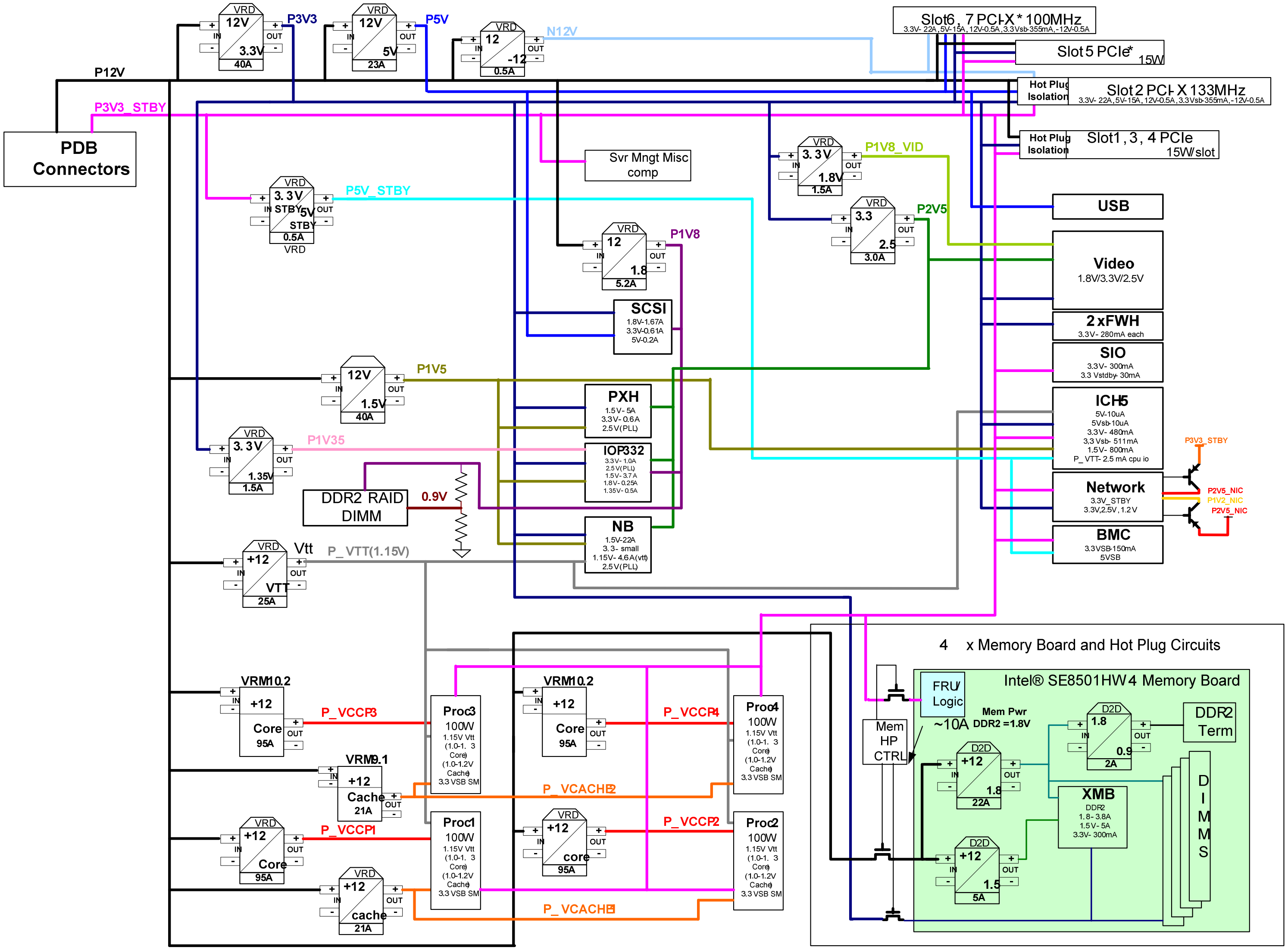


Figure 13. Power Distribution Block Diagram

Table 36. Power Budget

Subsystem	Qty	+12V	+3.3V$_{stby}$
Mainboard	1	147W	15W
Processors	4	448W	
Memory	16	192W	
PCI-X* slots	3	45W	
PCI Express* slots	4	80W	
Intel® Fibre Channel Module	1	15W	
Intel® Server Board Set SE8501HW4 Total		**927W**	**15W**

8.2 Power Timing

8.2.1 Power-Up Sequence

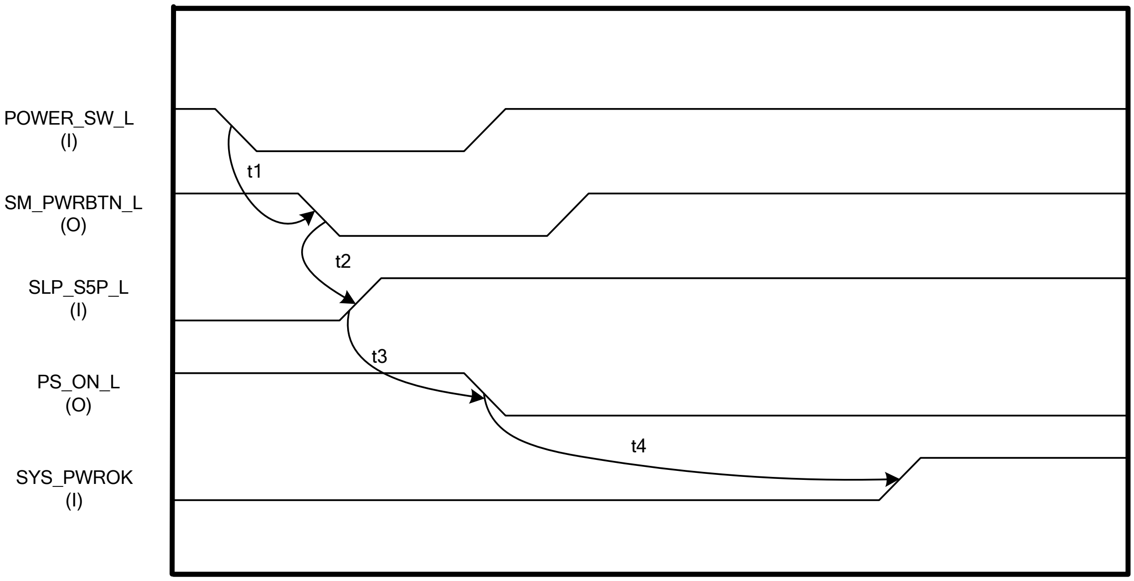


Figure 14. Typical Power-Up Sequence

Table 37. Typical Power-Up Timings

Reference	Description	Max	Typical	Min
t1	Time from front-panel power button push to BMC asserting the power button to the chipset. This includes the private store update for Pwr State change, which is on the order of 500ms + overhead, which accounts for other task completion time like Init Agent. BMC also debounces signal for 50ms.	2s	1s	50ms
t2	Time from BMC asserting power button to chipset, until chipset responds with SLP_S5.	–	16ms	60µs
t3	Time from when SLP_S5 is asserted, to when BMC asserts PS_ON_L to complete system power-on.	1s	97ms	50ms
t4	Time from when BMC has completed driving its power-on signals, to when system asserts power good back to BMC.	–	500ms	250ms

8.2.2 Power-Down Sequence

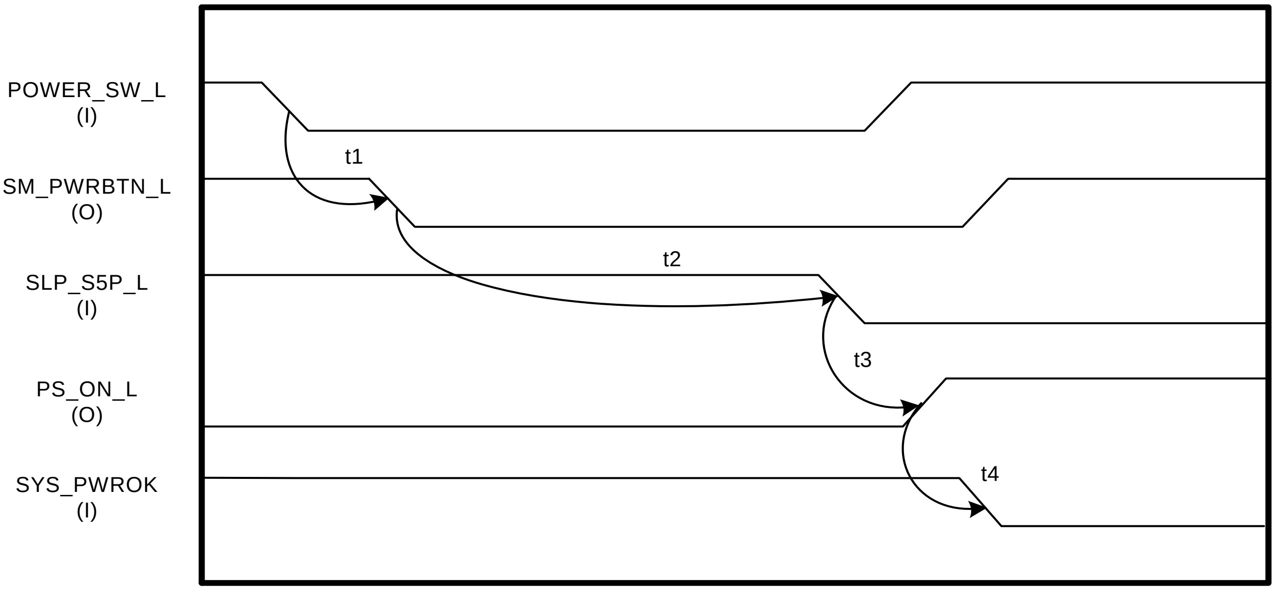


Figure 15. Typical Power-Down Sequence

Table 38. Typical Power-Down Timings

Reference	Description	Max	Typical	Min
t1	Time from front-panel power button push, to BMC asserting the power button to the chipset. BMC debounces the power button input for 50ms	1s	90ms	50ms
t2	Time from BMC asserting power button to chipset, until chipset responds with SLP_S5_L. Dependent on chipset setup.	5s	4.5s	–
t3	Time from when SLP_S5_L is asserted, to when BMC deasserts PS_ON_L to complete system power-off.	1s	160ms	50ms
t4	Time from BMC deasserting D2D enable, to when it deasserts PS_ON_L to complete system power-off.	–	100µs	0µs

8.3 Reset

Figure 16 and Table 39 illustrate the reset routing in the Intel® Server Board Set SE8501HW4.

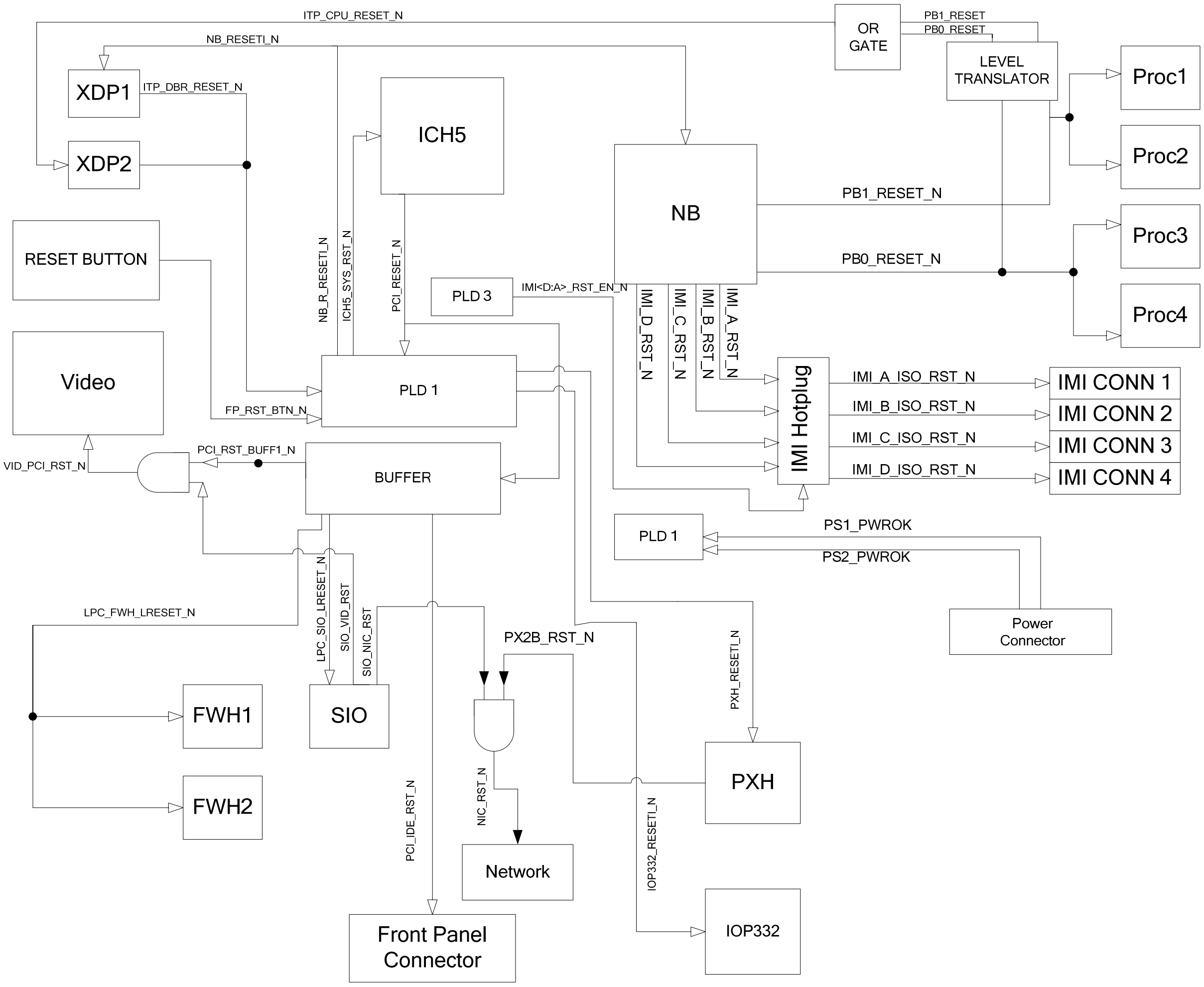


Figure 16. Reset Block Diagram

Table 39. Reset Types

Reset Type	Description
Front Panel Power Button	De-asserts PS_ON_L to the power supply and causes the system to shut down.
FP_RST_BTN_N ITP_RST	These signals are connected to the “Sources of Reset” logic inside the PLD. Any time any one of these signals is transitions LOW, the output of the logic SYS_ICH_RST asserts the SYS_RST_N to ICH5. Upon which ICH5 asserts PCI_RST_N back to PLD. Then PLD asserts the RESET# input to NB, PXH and Intel® IOP332 Storage I/O Processor.
NB_RST	This signal is controlled through the BIOS in ICH5.

8.4 Interrupts

The Intel® E8501 Chipset supports both XAPIC and 8259 interrupt delivery mechanisms. IOxAPIC controllers are located in the PXH, Intel® IOP332 Storage I/O Processor, and the ICH5. The 8259 controller is located in the ICH5. Figure 17 illustrates the interrupt routing in the Intel® Server Board Set SE8501HW4.

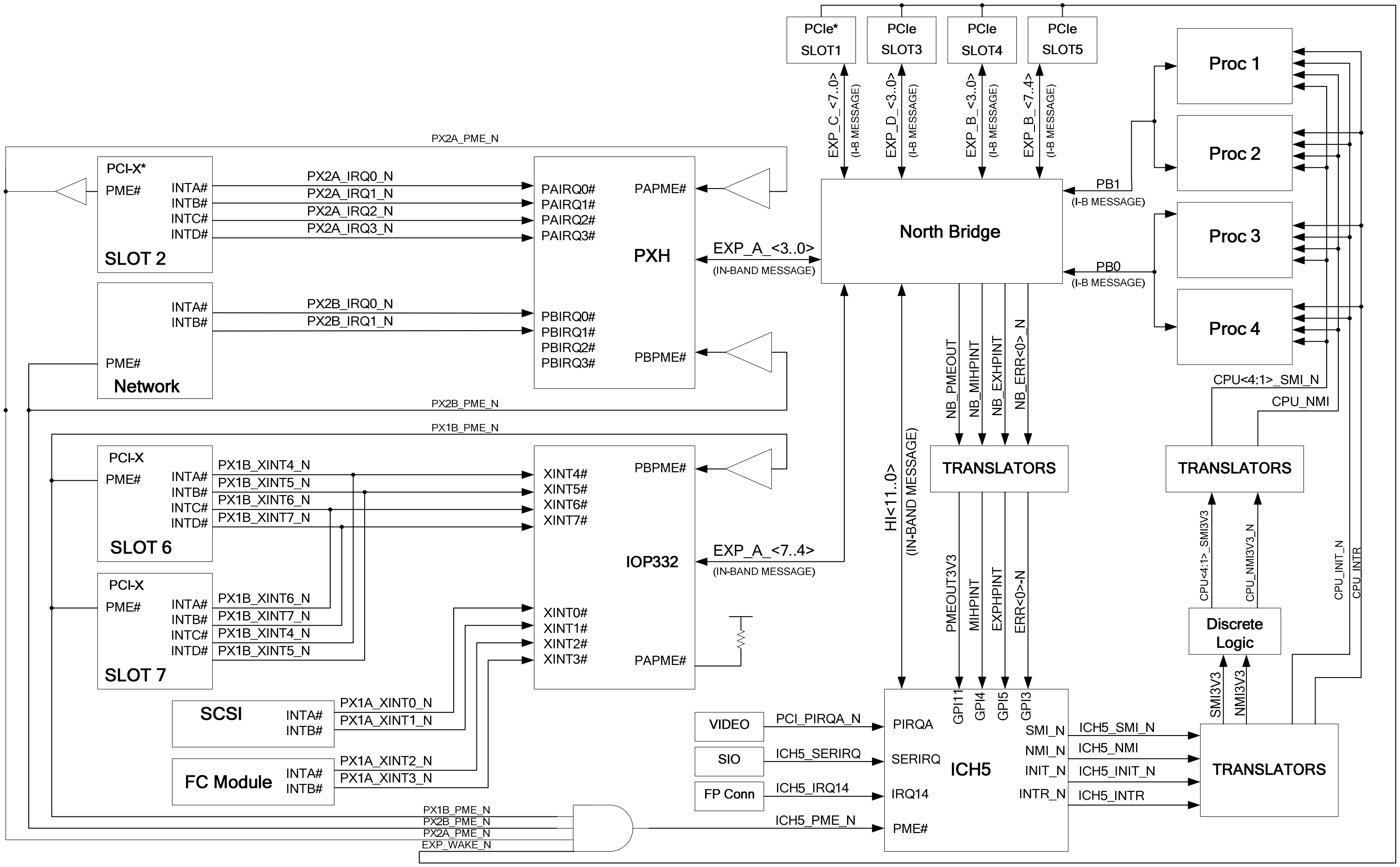


Figure 17. Interrupt Block Diagram

8.5 Clocks

The Intel® Server Board Set SE8501HW4 clock tree is generated from a single CK409 with spread spectrum capability. The CK409 generates multiple copies of differential pair high-speed clocks. Low skew DB800 buffers generate additional copies.

The FSB clocks must be length-matched. Skew control is also required on the 166MHz MPCLK going to the XMBs and NB, the 66MHz Hub link clocks, and the Legacy / LPC 33MHz clocks. Spread spectrum capability is enabled via an I^2C access to the CK409, which is connected to the ICH5's I^2C bus and controlled by the system BIOS.

8.6 Programmable Logic Devices

The Intel® Server Board Set SE8501HW4 has three Programmable Logic Devices (PLDs) for fundamental logic on the mainboard, including power, reset, hot-plug, and miscellaneous signaling. Due to the nature of these devices, they are not programmable by an end user.

Table 40. PLD Functions

PLD	Description
1	**System PLD:**
	Processor detection logic Power sequencing Reset Server management diagnostic LEDs
2	**BMC PLD:**
	Thermal management 32kHz clock generation PCI Express* Hot-Plug Clock debounce logic Power safety monitoring PLD-to-Server Management link
3	**IMI hot-plug PLD:**
	Support for memory board hot-plug events

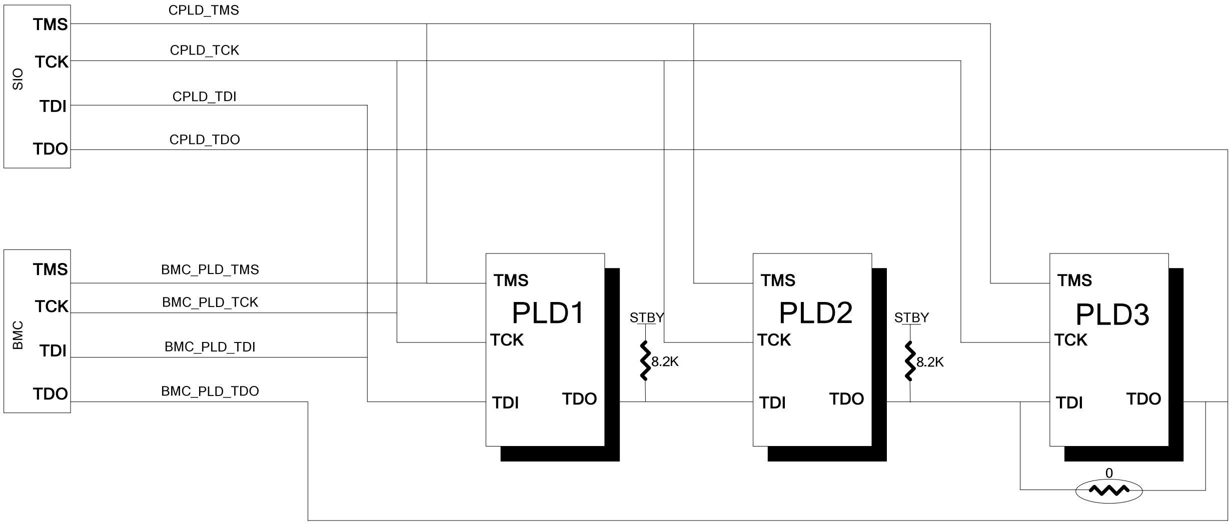


Figure 18. PLD Connections

9. Mechanical and Thermal Specifications

9.1 Mechanical Specifications

9.1.1 Mainboard

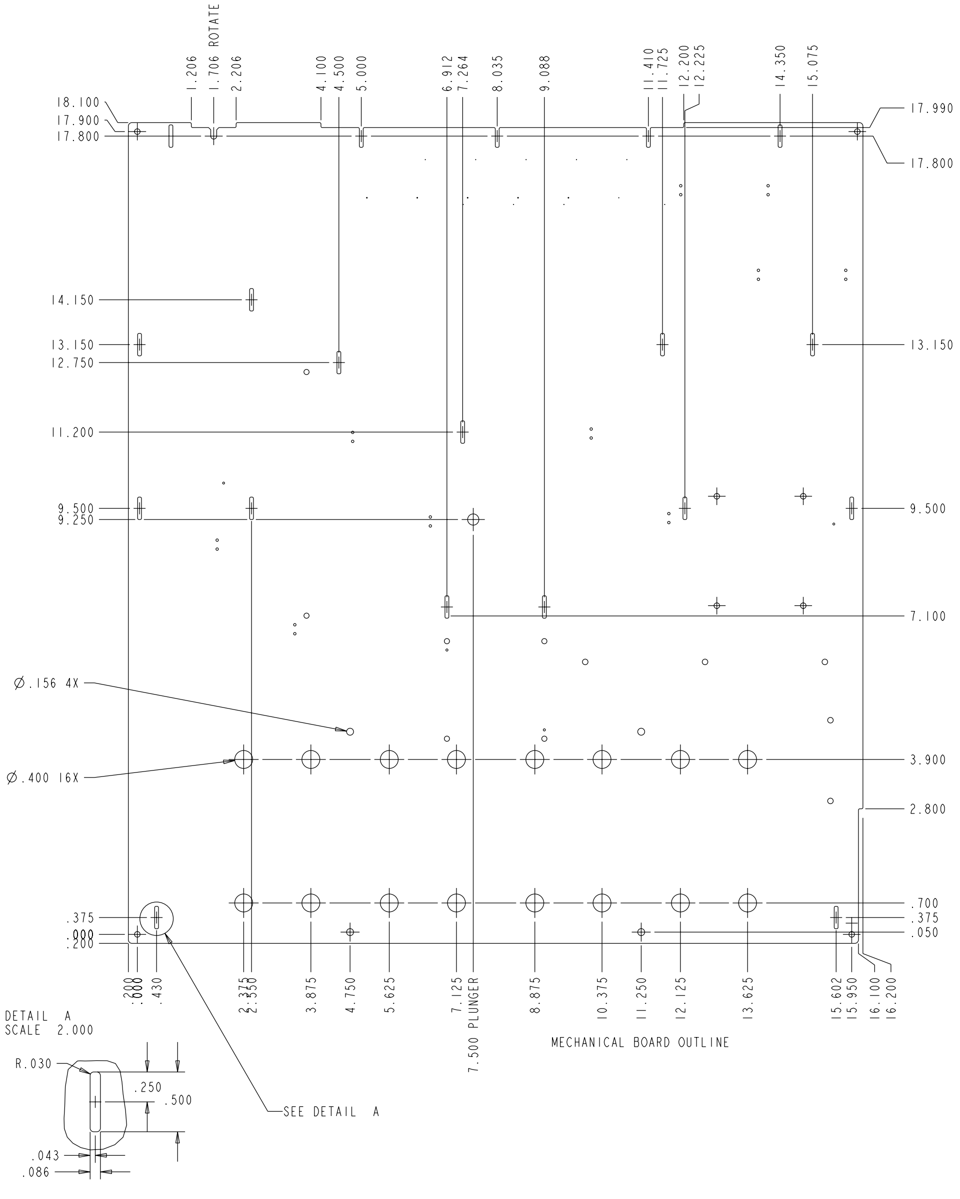


Figure 19. Mainboard Outline and Hole Location Drawing

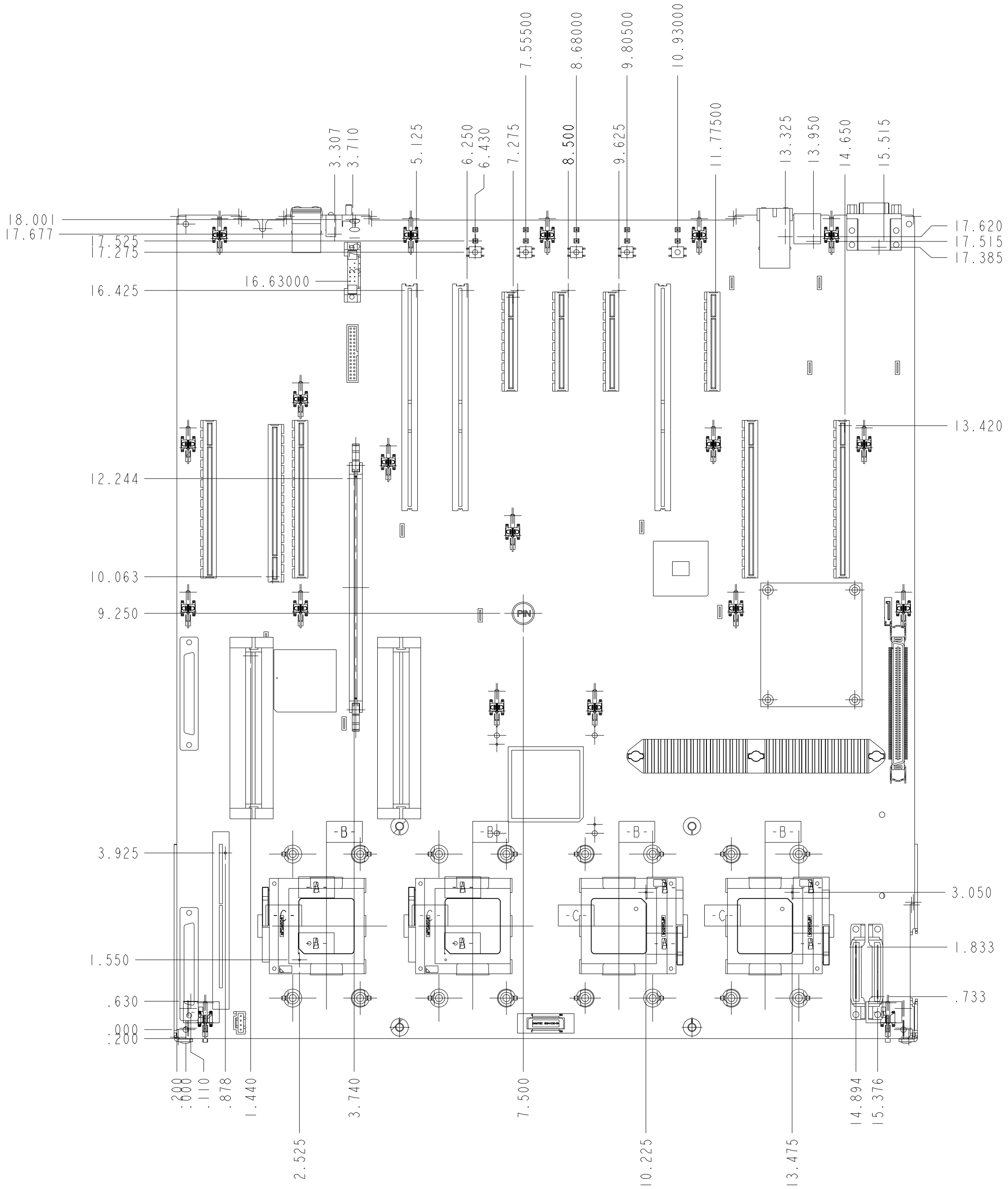
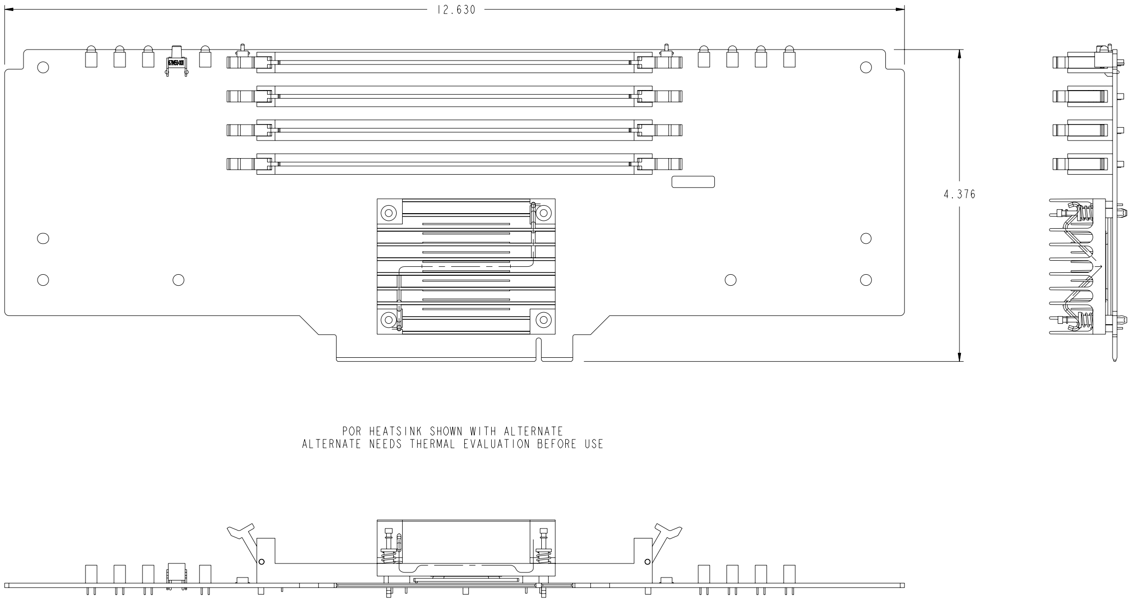


Figure 20. Mainboard Pin 1 Location Drawing

9.1.2 Memory Board



POR HEATSINK SHOWN WITH ALTERNATE
ALTERNATE NEEDS THERMAL EVALUATION BEFORE USE

Figure 21. Memory Board Mechanical Outline Drawing

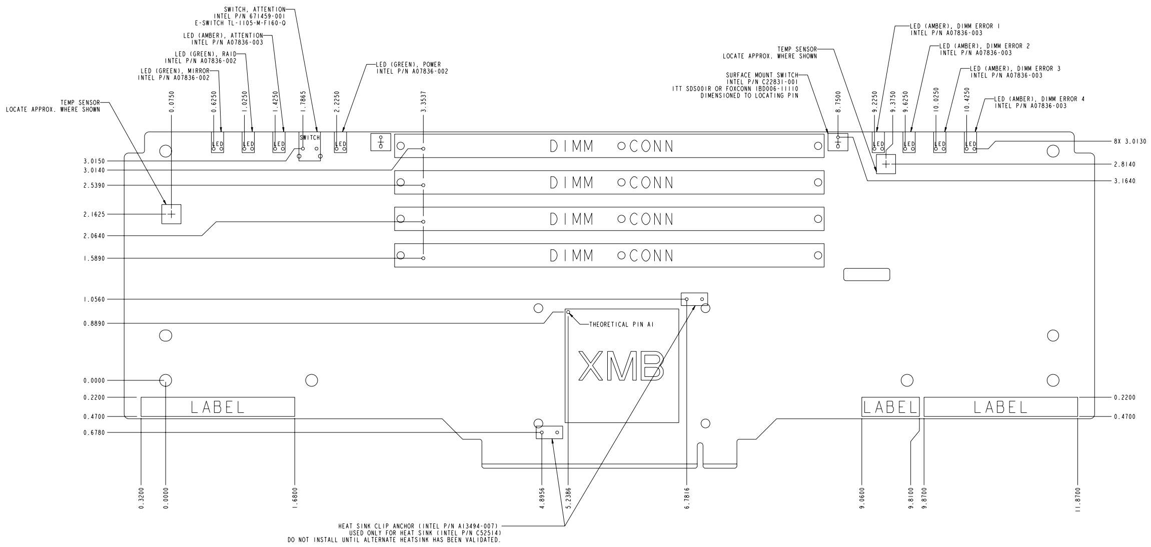


Figure 22. Memory Board Pin 1 Location Drawing

9.2 Thermal Specifications

Table 41. Thermal Specifications

Component	Target Velocity	Target Ambient	Temp Specification
Processors	See Processors Thermal Specifications		
Sockets	400 lfm	50 °C	100 °C, T_{socket}
Cache VRD	400 lfm	50 °C	90°C, T_{sink} @ MAX
Core VRD	400 lfm	50 °C	90°C, T_{sink} @ MAX
North Bridge	400 lfm	50 °C	105 °C, T_{HIS}
PXH	400 lfm	50 °C	105 °C, T_{die}
XMB	400 lfm	50 °C	105 °C, T_{case}
Intel® IOP332 Storage I/O Processor	400 lfm	50 °C	105 °C, T_{die}
ICH5	400 lfm	50 °C	85 °C, T_{case}
LSI* 53C1030 SCSI	400 lfm	50 °C	85 °C, T_{case}
ATI* Radeon* 7000 Video	400 lfm	50 °C	85 °C, T_{case}
Broadcom* BCM5704 Ethernet	400 lfm	50 °C	105 °C, T_{die}
DDR2 400MHz RAID DIMM	400 lfm	50 °C	85 °C, T_{case}
Mainboard	400 lfm	50 °C	100 °C, T_{board}

10. System BIOS

The system BIOS is implemented as firmware that resides in flash ROM. It provides hardware-specific initialization algorithms, basic input/output (I/O) services, and standard server board features. The flash ROM also contains firmware for certain embedded devices that are supplied by the device manufacturers and are not covered in this document.

The Intel® Server Board Set SE8501HW4 BIOS implementation is fully compliant to the Intel® Platform Innovation Framework for EFI architecture specifications. This Framework is a set of robust architectural interfaces that have been designed to accelerate the evolution of innovative, differentiated, platform designs. The Framework is Intel's recommended implementation of the EFI Specification for platforms based on all members of the Intel Architecture (IA) family.

A BIOS identification string is used to uniquely identify the revision of the BIOS being used on the system. The following is an example BIOS identification string:

SHW40.86B.P01.01.00.0001.031820051839

- Board ID, ‘SHW40’ for Intel® Server Board Set SE8500HW4 or the Intel® Server Board Set SE8501HW4
- OEMID, ’86B’ is used for Intel Server Boards
- Build type and version, ‘P01’ for production version 1
- Major revision, ‘01’
- Minor revision, ‘00’
- Build ID, ‘0001’
- Build date and time, March 18, 2005 at 18:39

10.1 Advanced Memory Modes

The Intel® Server Board Set SE8501HW4 supports several memory features that allow flexibility in performance, redundancy, and the ability to upgrade. The system BIOS can be configured for maximum performance as follows:

- Where memory is up to four-way interleaved; maximum compatibility
- Where memory can be hot-added; memory mirroring
- Where two or four boards are used to keep a copy of system memory; memory RAID
- Where four boards are used in a RAID4-like mode

Only one of these memory modes can be selected at one time, and the BIOS defaults to maximum performance mode. For the non-redundant modes, support is also included for memory sparing, where a portion of each memory board is reserved for failover.

Hot-replace means the user can replace a memory board with another memory board of identical total size. This operation is supported in memory RAID and memory mirroring modes.

Hot-add means the user can add a memory board to a previously unoccupied slot. This requires operating system support and is supported in maximum compatibility and memory mirroring modes.

Hot upgrade means the user can replace an existing memory board with a memory board that contains more memory capacity. This requires operating system support and is supported by the memory RAID mode only.

Table 42. Memory Hot-Plug Support Under Different Memory Modes

Memory Hot-Plug Operation	Maximum Compatibility	Maximum Performance	Memory Mirroring	Memory RAID
Hot-add	Supported		Supported	
Hot-replace			Supported	Supported
Hot-upgrade				Supported

10.1.1 Sparing

Sparing allows memory to be set aside to replace memory under use when a DIMM's correctable error count has reached a specified threshold. Unlike mirror or RAID configurations, spared memory configurations do not provide redundant copies of memory and the system cannot continue to operate when an uncorrectable error occurs.

DIMMs in the Intel® Server Board Set SE8501HW4 are installed in pairs, and are referred to as a bank, DIMM_1B and DIMM_1A form one bank, while DIMM_2B and DIMM_2A form another. A DIMM pair may consist of one rank or two ranks. When the memory mode is maximum performance or maximum compatibility, the BIOS Setup supports setting one rank aside to serve as a spare for each memory board. When the correctable error rate for a failing rank exceeds the error threshold for switching to spare, the contents of the failing rank are copied to the spare rank. At the completion of the copy, the failing rank is disabled and the spare rank is used in its place. The BIOS reports the failing rank with a SEL event, updates the DIMM error LED on the memory board, and sends memory RAS commands to the BMC to update the system memory state. The DIMMs with the failed rank are disabled on subsequent boots. The spare rank is no longer used for spare, but instead used as system memory.

When the BIOS Setup is configured for sparing, the largest rank is chosen to serve as the spare. This ensures that the contents of any failing rank fit on the spare rank. The amount of available memory in the system is reduced by the size of the spare rank. If only one rank is available on a memory board, the system BIOS does not configure this rank as a spare.

Table 43. Memory Modes Supporting Sparing

Memory Mode	Support For Sparing
Maxium Compatibility	Yes
Maxium Performance	Yes
Memory Mirroring	No
Memory RAID	No

10.1.2 Maximum Compatibility

The maximum compatibility mode allows the most flexibility in installing DIMMs and memory boards and allows memory boards to be hot added. This memory mode is one-way interleaved, allows sparing configuration, but results in the lowest performance of the supported configurations.

10.1.3 Maximum Performance

The maximum performance mode is the default memory configuration and provides the best performance. With four memory boards installed, the BIOS configures memory as four-way interleaved, across all the memory boards. With less than four memory boards installed, the BIOS attempts to configure two-way interleaving. If memory cannot be configured for two-way interleaving, the BIOS defaults to one-way. This memory mode allows sparing configuration but does not support any memory board hot-plug operations.

10.1.4 Memory Mirroring

The mirror memory mode requires either two or four same size memory boards and provides redundancy at the cost of halving the effective memory size. The mirror configuration allows for the hot replacement of an existing board for a board containing an equal amount of memory or the hot addition of two memory boards to a pair of empty memory board slots only.

A pair of memory boards in memory mirror mode forms a redundant group. One of the memory boards is designated the primary image and the other the secondary image. For memory writes, the write request is issued to both boards. For memory reads, the read request is issued to the primary memory board. In the event of a detected correctable error, the primary image toggles and the read is issued to the previous secondary image. In the event of a detected uncorrectable error, the primary and secondary images switches with each other and the failed image cannot become the primary image again until the failed DIMMs have been replaced and the image re-built. The first redundant group consists of memory board A mirrored with memory board B. The second redundant group consists of memory board C mirrored with memory board D. The BIOS sets the memory board mirror LED to indicate that the memory board is operating in the memory mirror mode.

Supported memory board configurations for memory mirroring mode are:

- Memory board A mirrored with memory board B, both of equal size
- Memory board C mirrored with memory board D, both of equal size
- Memory board A mirrored with memory board B, both of equal size; **and** memory board C mirrored with memory board D, both of equal size.

Memory board hot replace is supported in the following way:

- Memory board A mirrored with memory board B, both of equal size. Remove memory board A or B and replace with an equal sized memory board
- Memory board C mirrored with memory board D, both of equal size. Remove memory board C or D and replace with an equal sized memory board

The memory board hot add is supported in the following way:

- Memory board A and B previously installed with memory board slots C and D empty. Equal sized memory boards can be installed in slot C then D, one at a time.
- Memory board C and D previously installed with memory board slots A and B empty. Equal sized memory boards can be installed in slot A then B, one at a time.

10.1.5 Memory RAID

The memory RAID mode requires four same-size memory boards and provides redundancy at the cost of quartering (¼) the effective memory size. Memory RAID mode acts similar to the Redundant Array of Inexpensive Disks (RAID) level 4, where data is striped across three memory boards and parity information is kept on the fourth.

When one board fails, the memory subsystem operates in non-redundant mode. The data from the remaining three boards is used to reconstruct the data that was on the failed memory board. When the failed memory board location is hot replaced, the BIOS rebuilds the RAID by reconstructing the data that was on the previously failed memory board and writes the data to the newly installed board. When the re-build is complete, the system is once again in redundant mode. The BIOS sets the memory board RAID LED to indicate that the memory board is operating in the memory RAID mode.

Memory hot upgrade is performed with the following steps:

1. In the BIOS Setup confirm the RAID Upgrade Gap size. The gap is the same size as the memory BIOS allocated on each memory board for the RAID memory capacity addition.
2. Hot remove one memory board.
3. Upgrade the removed board, with the gap size determined in the BIOS Setup
4. Hot add the higher capacity memory board
5. Repeat Steps 2-4 with the remaining three memory boards.
6. When the last memory board has been upgraded, BIOS then sends an ACPI notification of the new memory size to the operating system.

Supported memory board configurations for this mode are:

- Memory boards A, B, C and D are all of equal size.
- The memory board hot replace is supported in the following way:
- Memory boards A, B, C and D are installed and are of equal size. Remove the memory boards A, B, C, or D and replace with an equal sized memory board.

The memory board hot upgrade is supported in the following way:

- Memory boards A, B, C and D are installed and of equal size. The BIOS Setup has been configured with a RAID Upgrade Gap size corresponding to the planned size update. One at a time, remove memory boards A, B, C, and D and replace with an updated size (that does not exceed the RAID Update Gap size) of the memory board.

10.2 Rolling BIOS

The Intel® Server Board Set SE8501HW4 BIOS can be updated while the server is online, as opposed to immediately turning off the server after a BIOS update. This rolling BIOS features are supported by having two copies of the BIOS, the one in use, and a secondary copy to which an updated BIOS version can be written. When ready, the system can roll forward to the new BIOS. In case of a failure with the new version, the system can roll back to the previous version. The Intel® Server Board Set SE8501HW4 does not automatically use the new BIOS. To move to the new BIOS the system must be rebooted.

The Firmware Hub (BIOS flash) is divided into two partitions: primary and secondary. The active BIOS partition that the system boots from shall be referred to as the primary partition. The BIOS updates are written to the secondary partition. After the update, a notification flag is set, and the after subsequent boot following the BIOS update, the system boots from the new primary BIOS partition. If the new BIOS fails to boot, specialized hardware switches back to the BIOS on the other partition, thus affecting a “roll back”. The BMC logs events associated with the BIOS updates to the SEL.

10.3 Initialization

10.3.1 Processors

The Intel® Server Board Set SE8501HW4 has two processor front-side buses, each accommodating two processors. At reset, hardware arbitration chooses one Boot Strap Processor (BSP) per FSB. However, the BIOS POST code requires only one processor for execution. This requires the BIOS to elect a “system BSP” using registers in the NB. The BIOS cannot guarantee which processor is the system BSP, only that a system BSP is selected. From this point forward, the system BSP is referred to as just the BSP.

The BSP is responsible for executing the BIOS power-on self-test (POST) and preparing the machine to boot to an operating system. At boot time, the system is in virtual wire mode and the BSP alone is programmed to accept local interrupts (INTR driven by programmable interrupt controller) and non-maskable interrupt (NMI)).

As a part of the boot process, the BSP wakes each Application Processor (AP). When awakened, an AP programs its Memory Type Range Registers (MTRR) to be identical to those of the BSP. All APs execute a halt instruction with their local interrupts disabled. If the BSP determines an AP exists, with a lower-featured processor, or a lower value returned by the CPUID function, the BSP switches to the lowest-featured processor in the system. This algorithm is described in [IA-32_BWG]. The System Management Mode (SMM) handler expects all processors to respond to a Server Management Interrupt (SMI).

See Section 5.4 for more information on the BIOS and BMC interaction during the initial fault resilient booting process.

An FRB3 failure is recorded automatically by the BMC and the AP failures are logged to the SEL by the BIOS.

The BMC maintains a failure history for each processor in nonvolatile storage. There are three possible states for each processor slot:

- Processor installed (Status only, indicates processor has passed the BIOS POST)
- Processor failed The processor may have failed FRB3, and has been disabled
- Processor not installed (Status only, indicates the processor socket has no processor)

Once a processor is marked failed, it remains marked failed until “Processor Retest” option is chosen in the BIOS Setup. The BIOS displays an informational message on the console to remind the user about a previous processor failure until all processors have been retested and successfully pass FRB and AP initialization. If all the processors are marked failed, the system does not alter the BSP and attempts to boot from the original BSP. In the case of a failure, the BIOS displays and error message on the console and the logs the errors in the system event log.

If the user replaces a processor that has been marked failed by the system, the system must be informed about this change. Selecting the “Processor Retest” option in the BIOS Setup causes all processors to be retested.

10.3.1.1 Mixed Processor Steppings

For optimum system performance, only identical processors should be installed in a system. Processor steppings can be mixed in a system provided there is no more than a one stepping difference in all processors installed. If the installed processors are more than one stepping apart an error is reported. Acceptable mixed steppings are not reported as errors by the BIOS.

10.3.1.2 Unsupported Processor Configurations

In the following configurations, the BIOS reports an error:

- BIOS detects a processor for which a microcode update is not available
- Mixed processor models are installed
- Mixed processor families
- Mixed processor cache sizes. The size of all cache levels must match between all installed processors.

10.3.1.3 Jumperless Processor Speed Settings

The 64-bit Intel® Xeon® processors MP do not utilize jumpers or switches to set the processor frequency. The BIOS reads the highest ratio register from all processors in the system. If all processors are the same speed, the actual speed is the highest speed probed. If not all processors match, the highest common value between high and low ratio is determined and programmed for all processors. If there is no value that works for all installed processors, all processors not capable of speeds supported by the BSP are disabled and an error is displayed.

10.3.1.4 Microcode Update API

Modern Intel processors have the capability of correcting specific errata through the loading of an Intel-supplied data block (i.e. microcode update). The BIOS is responsible for storing the update in nonvolatile memory and loading it into each processor during POST. The BIOS allows a number of microcode updates to be stored in the Flash, limited by the amount of free space available. The BIOS performs the recommended update signature verification prior to storing the update in the Flash. The system BIOS supports the real mode INT 15, D042 interface for updating the microcode updates in the flash.

10.3.1.5 Hyper-Threading Technology

64-bit Intel® Xeon® processors MP support Hyper-Threading Technology. By default, the BIOS detects processors that support this feature and enable it during POST. The BIOS Setup provides an option to selectively enable or disable this feature.

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

Because some operating systems are not able to efficiently utilize the Intel Hyper-Threading Technology, the BIOS does not have entries in the MP tables to describe the virtual processors.

10.3.1.6 Intel SpeedStep® Technology

64-bit Intel Xeon Processors MP support the Geyserville3 (GV3) feature of Intel SpeedStep® Technology. This feature changes the processor operating ratio and voltage similar to the Thermal Monitor 2 (TM2) feature. It must be used in conjunction with the TM1 or TM2 feature. The Intel® Server Board Set SE8501HW4 supports the GV3 feature in conjunction with TM2 feature.

10.3.1.7 Intel® Extended Memory 64 Technology

The Intel® Server Board Set SE8500HW4 BIOS supports Intel® Extended Memory 64 Technology (Intel® EM64T) for executing both 32-bit and 64-bit applications simultaneously.

10.3.2 Memory

ECC memory must be initialized by the BIOS before it can be used. The BIOS executes a hardware memory test before configuring memory during POST and during runtime when a memory board is hot inserted to the system. The memory test can be enabled or disabled based on a BIOS setup option. During POST, the hardware memory test is executed in parallel on all memory boards before video is available. Hardware memory testing tests every byte of memory location and cannot be stopped once initiated. The hardware isolates an uncorrectable error down to a DIMM pair and a correctable error to a DIMM.

When the memory initialization test encounters bad DIMM(s), it disables the bad DIMM(s) and turns on the corresponding DIMM error LED indicator on the memory board. The BIOS also reports the correctable or uncorrectable error on the bad DIMM(s) and that the bad DIMM and its bank partner DIMM has disabled. If bad DIMM(s) from the memory test results in the BIOS not being able to set the desired configuration during POST, the BIOS reports this error and continues booting with the maximum performance configuration.

During a hot insertion operation, if the bad DIMM(s) from the memory test results in the system not being able to set the desired memory mode during runtime, the BIOS rejects the new memory board addition request and powers down the newly inserted board.

After the BIOS successfully executes the hardware memory test, it zeros out the contents of memory. The BIOS also sends BMC memory RAS commands to update the system memory state.

10.3.2.1 Disabling Failed Memory

The BIOS and chipset disable memory when one of the following occurs:

- The initialization locates a bad DIMM and disables the DIMM bank.
- An uncorrectable ECC error has occurred on a DIMM during runtime. The BIOS disables the DIMM bank for subsequent boots.
- A DIMM rank surpasses an error threshold for switching to spare during runtime. Hardware disables the DIMM rank after its contents are copied to a spare rank. The BIOS disables the DIMM bank for subsequent boots.
- A failed memory board is disabled by the system hardware and the BIOS.

On subsequent boots, the disabled memory is not initialized the DIMM error LED relights after system initialization. If all memory in a system has been disabled, the BIOS generates beep codes to indicate that the system has no usable memory.

Disabled memory may be re-enabled and retested by enabling the setup option for “Retest All System Memory” or “Retest Board Memory”. “Retest All System Memory” re-enables initialization and test of all memory boards and slots whereas “Retest Board Memory” re-enables and retests only the slots on the desired board.

The BIOS records the disabled memory to the SEL.

10.3.2.2 Handling ECC Errors and XMB Fail During Runtime

The BIOS handles ECC errors based on whether the error is correctable or uncorrectable and if the current memory mode is redundant. A RAID configuration with all good memory boards operates in redundant mode. A redundant group in a mirror configuration is redundant if each of its boards operates in redundant mode. The maximum performance and maximum compatibility modes operate in a non-redundant state. RAID configurations and mirror board pairs with failed or missing memory boards also operate in a non-redundant state.

If the system is operating in a non-redundant state during runtime and an uncorrectable ECC error occurs the BIOS reports the error to the SEL, sets the memory board LED to indicate a bad DIMM and disables the DIMM(s) for subsequent boots. The BIOS triggers a non-maskable interrupt to halt the system.

If the system is operating in a redundant state during runtime and an uncorrectable ECC error occurs, hardware marks the bad memory location and the system continues to function by reading from the redundant copy of memory. Additionally, the BIOS ECC error handler increments the DIMM bank's uncorrectable error count, if the error count is less than ten per hour, the BIOS reports the uncorrectable ECC error to the SEL. When the DIMM uncorrectable error count reaches 10, BIOS illuminates the bad DIMMs LEDs and disables the DIMM bank for subsequent boots. The system continues to function from redundant memory.

Multiple consecutive uncorrectable ECC errors may cause an XMB fault condition and the entire memory board to be disabled. When an XMB fault occurs, the BIOS is no longer able to access the XMB registers in order to locate the failing DIMM(s). Hence, BIOS does NOT illuminate the bad DIMM LED, nor log the failed DIMM information or disable the failed DIMM(s).

If XMB faulted due to uncorrectable ECC errors while system is operating in a redundant state, the system continues operation in a non-redundant state. The BIOS logs a SEL event to indicate that an uncorrectable ECC error has occurred on the faulted memory board. In this condition, the BIOS also sends commands to the BMC to update the DIMM(s) state as "Not Present". The user may perform a memory hot replace operation to replace the bad memory board with a known good memory board to restore the system to redundant mode.

If multiple uncorrectable ECC errors occur while the system is operating in non-redundant mode, the system may hang.

When a correctable ECC error occurs during runtime, the DIMM correctable error count is incremented. If the error count is less than the error stop report threshold, the BIOS reports the correctable ECC error to the SEL. If the board containing the DIMM with the correctable error has available spares, the error stop report threshold shall be the same as the error threshold for switching to spare. If the board has no available spare, the error stop report threshold shall be ten errors per hour. When the error count reaches the error stop report threshold, the BIOS reports to the SEL that the correctable error stop report threshold has been reached and stops reporting of subsequent correctable ECC errors for the DIMM. The following occurs if a spare rank is available on the memory board on which the error is located, and the error threshold for switching to the spare is reached:"

1. The system copies the contents of the bad rank to the spare rank.
2. The system switches to the spare rank.
3. Sets the memory board LED to indicate the bad DIMM(s).
4. Disables the bad DIMM bank and sparing for subsequent boots.

With sparing disabled, the ranks previously reserved for spares are used for system memory.

Any disabled event reporting is re-enabled on the next reboot.

10.3.3 Operating System

The Intel® Server Board Set SE8501HW4 BIOS provides an OS Boot Timer that acts after the processor FRB stages have completed. By enabling this timer option in the BIOS Setup, the system BIOS enables a timer in the BMC with the requested number of minutes. The OS Boot Timer option is disabled by default. It is the responsibility of the operating system, or application, to disable this timer once it has successfully loaded.

NOTE: Enabling the OS Boot Timer without having an operating system or server management application installed that supports the timer feature will cause the system to reboot when the timer expires. Refer to operating system documentation to confirm this timer feature is supported.

10.4 Remote Management

The BIOS supports redirection of both video output and keyboard input via a serial link (COM port). When console redirection is enabled, local (host server) keyboard input and video output are passed both to the local keyboard and video connections and to the remote console via the serial link. Keyboard inputs from both sources are considered valid and video is displayed to both outputs. Optionally, the system can be operated without a host keyboard or monitor attached to the system and run entirely via the remote console. Setup and any other text-based utilities can be accessed via console redirection.

10.4.1 Serial Configuration Settings

When redirecting input/output through a modem (as opposed to a null modem cable), the modem needs to be configured with the following:

- Auto-answer (for example, ATS0=2, to answer after two rings).
- No parity, 8-bit data, 1 stop bit (N, 8, 1 mode)
- Modem reaction to DTR set to return to command state (e.g., AT&D1).

Not setting the second item results in the modem either dropping the link when the server reboots (if AT&D0) or becoming unresponsive to server baud rate changes (if AT&D2).

The option for handshaking must be set to CTS/RTS + Carrier Detect (CD) for optimum performance. If EMP is sharing the COM port with serial redirection, the handshaking must be set to Xon/Xoff + CD. With this form of handshaking, the server is prevented from sending video updates to a modem that is not connected to a remote modem. If this is not selected, video update data being sent to the modem inhibits many modems from answering an incoming call. An EMP option utilizing CD should not be used if a modem is not used and the CD is not connected.

The BIOS supports multiple consoles, some of which are in graphics mode and some in text mode. The graphics consoles display the splash logo while the text consoles receive the redirected text.

The console redirection ends at the beginning of the Legacy OS boot (INT 19h).

The remote console refresh rate depends on the selected Baud rate.

10.4.2 Keystroke Mappings

During console redirection, the remote terminal (which may be a dumb terminal or a system with a modem running a communication program) sends keystrokes to the local server. The local server passes video back over this same link. The keystroke mappings follow VT-UTF8 format with the following extensions.

10.4.2.1 Setup Alias Keys

The <Del> and <Ctrl>-<F> key combinations are synonyms for the <F2> or "Setup" key. They are implemented, but do not appear in prompted screen messages. These hotkeys are only defined for console redirection support, and do not work for locally attached keyboards.

10.4.2.2 Standalone <Esc> Key for Headless Operation

The Intel® Server Board Set SE8501HW4 BIOS is configured to support the *Microsoft Headless Design Guidelines*, which describe a very specific implementation for the <Esc> key as a single standalone keystroke:

- <Esc> followed by a two-second pause must be interpreted as a single escape.
- <Esc> followed within two seconds by one or more characters that are not forming a sequence described in this specification must be interpreted as <Esc> plus the character or characters, not an escape sequence.

When enabled in the BIOS Setup, and sent from a remote terminal, the key sequence "<Esc>R<Esc>r<Rsc>R" performs a Remote Console Reset.

10.4.3 Limitations

The BIOS console redirection terminates after an EFI-aware operating system calls EFI boot service ExitBootServices. The operating system is responsible for continuing the console redirection after this point.

The BIOS console redirection is a text console and any graphical data, such as a logo, are not redirected.

10.4.4 Interface to Server Management

If the BIOS determines that console redirection is enabled, it reads the current baud rate and passes this value to the appropriate management controller via the IPMB.

10.5 IPMI Serial/Modem Interface

The BMC controls whether the COM2 internal connector is electrically connected to the BMC or the standard serial port of the SIO. Refer to the *IPMI 2.0 Specification* for more information, with Intel® Server Board Set SE8501HW4 specific implementation described in this section.

10.5.1 Channel Access Modes

The BIOS supports the four different channel access modes described in the *IPMI 2.0 Specification*.

10.5.2 Interaction with BIOS Console Redirection

The BIOS console redirection uses VT-UTF8 console redirection support. This implementation was chosen to meet the functional requirements. The requirements are set forth in the Microsoft Windows 2003* WHQL requirements for headless operation of servers. It was also chosen to maintain a necessary degree of backward compatibility with existing Intel server BIOS products.

The server BIOS has a console that is intended to interact with a display and keyboard combination. The BIOS instantiates sources and sinks of input/output data in the form of BIOS Setup screens, Boot Manager Screens, Power On Self Test (POST) informational messages, and hotkey/escape sequence action requests.

Output is displayed locally on video display devices, currently limited to VGA displays in text or graphics mode. Input locally may come from a USB keyboard, without mouse support.

The use of serial port console redirection allows a single serial cable to be drawn in for each server system. Then the serial cables from a number of servers can be connected to a serial concentrator or to a switch, which allows access to each server system individually. The system administrator can switch from one server to another to manage large numbers of servers without having to physically interact with the individual servers.

10.5.3 Serial Over LAN

The BIOS automatically starts console redirection on COM2 if it detects SOL is enabled in the BMC. The BIOS sets COM2 flow control and baud rate from BMC's IPMI Serial/Modem configuration. Data bits are set to eight bits/character, no parity and one stop bit as per IPMI messaging requirement, and the console type is set to VT100+.

BIOS console redirection on COM2 supports an extra control escape sequence to force the COM2 port to the BMC. After this command is sent, the COM2 port attaches to the BMC channel access serial port and the SIO COM2 data is ignored. This feature allows a remote user to monitor the status of POST using the standard BIOS console redirection features and then takes control of the system reset or power using the channel mode features. If an error occurs during POST, a watchdog time-out feature in the BMC automatically takes control of the COM2 port.

10.6 Wired For Management

Wired for Management (WFM) is an industry-wide initiative to increase overall manageability and reduce total cost of ownership by allowing a server to be managed over a network. To meet WFM requirements, the system BIOS supports the *System Management BIOS Reference Specification*.

10.6.1 PXE BIOS Support

The BIOS supports EFI PXE implementation with the Universal Network Device Interface driver included on the network card. The BIOS also supports Legacy PXE option ROMs in Legacy mode. The Legacy PXE ROM is required to boot a non-EFI operating system over the network.

10.7 System Management BIOS

There are two access methods defined for the System Management BIOS (SMBIOS) structures. The Intel® Server Board Set SE8501HW4 BIOS supports the table access method, where accessing SMBIOS structures can be accessed under 32-bit protected-mode operating systems. The PnP function interface is not supported by the Intel® Server Board Set SE8501HW4 BIOS.

The total number of structures can be obtained from the SMBIOS entry-point structure. The system information is presented to an application as a set of structures that are obtained by traversing the SMBIOS structure table referenced by the SMBIOS entry-point structure. Please refer to the *System Management BIOS Reference* for more information.

10.8 Security

The Intel® Server Board Set SE8501HW4 BIOS can use two different levels of password security to prevent unauthorized use of the system. Setting a user password allows for modification of only the time, date, language and the user password. Setting an administrator password allows full access to all setup fields. An administrator password should be set and saved, before a user password can be set. The maximum length of the password can have up to seven alphanumeric characters (a-z, A-Z, 0-9) and is not case sensitive.

Once set, a password can be cleared by changing it to an empty value. If only one password is set, this password is required to enter the BIOS Setup.

If the administrator password is cleared, the user password is also cleared. Passwords are not enabled until the next reboot.

If the user enters three consecutive wrong passwords during the boot sequence, the system is placed into a halt state. A system reset is required to exit out of the halt state. This feature makes it difficult to break the password by “trial and error” method.

If the user or administrator password(s) are lost, both passwords may be cleared by moving the password clear jumper into the “clear” position. The BIOS determines if the password clear jumper is in the “clear” position during the BIOS POST and, if required, clears both passwords. The password clear jumper must be restored to its original position before a new password(s) can be set.

11. BIOS User Interface

11.1 Overview

There are two types of consoles used for displaying the user interface, graphical or textual. Graphics consoles are in 800x600 mode (pixels). Text consoles are 80 characters x 25 lines.

Console output is partitioned into three areas, the System Activity/State, Logo/Diagnostic, and Current Activity windows. The System Activity Window displays information about the current state of the system. It provides indication to the user if the system is active, hung, or requires user intervention. The Logo/Diagnostic Window displays the OEM splash screen logo or a diagnostic screen. The Current Activity Window displays information about the currently executing portion of POST as well as user prompts or status messages.

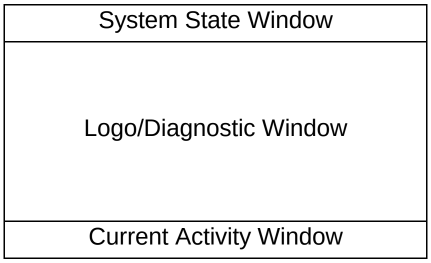


Figure 23. BIOS Display

11.1.1 System State Window

The top row of the screen is reserved for the system state window. On a graphics console, the row is 800x19. On a text console, the row is 80x1.

The system state window may be in one of three forms, either an activity bar that scrolls while the system is busy, a progress bar that measures percent complete for the current task, or an attention-required bar. The attention bar is useful for tasks that require user attention to continue.

11.1.2 Logo/Diagnostic Window

The middle portion of the screen is reserved for the logo/diagnostic window. On a graphics console, the screen is 800x486. On a text console, the window is 80x19.

The logo/diagnostic window may be in one of two forms; either a logo splash screen is displayed, in Quiet Boot mode, or a system summary and diagnostic screen is displayed, in verbose mode. The default is to display the logo in Quiet Boot mode. If no logo is present in the flash ROM, or Quiet Boot mode is disabled in the system configuration, the summary and diagnostic screen is displayed. During a Quiet Boot, if the user presses <Esc>, the system transfers from the logo screen to the diagnostic screen.

11.1.3 Current Activity Window

The bottom portion of the screen is reserved for the current activity window. On a graphics console, the screen is 800x95. On a text console, the window is 80x5.

11.2 System Diagnostic Screen

The diagnostic screen is the console area where boot information, options, and diagnostic utilities are displayed. All built in utilities use this area in a similar manner to provide for consistent user interaction. The system diagnostic screen is divided into four areas:

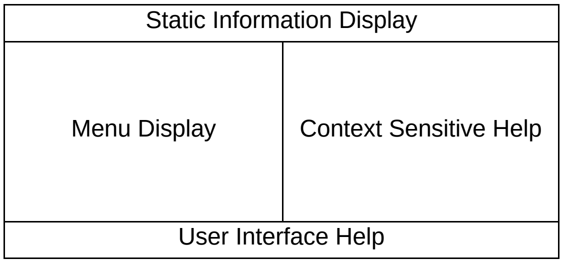


Figure 24. System Diagnostics Display

The static information display contains basic information about the system, including copyrights and the BIOS ID.

The menu display area contains menu-driven access to system options and utilities. This includes Boot Manager, Boot Maintenance Manager for managing boot options/devices/files, BIOS Setup Utility and Error Manager. Options can be highlighted using the up and down arrow keys and the current highlighted option can be executed by pressing the <Enter> key.

The context sensitive help area displays user oriented information specific to the currently highlighted option in the menu display area.

The user interface help area displays information about navigation keys based on the current menu in the menu display area.

11.3 Systems Options Menu Screen

Table 44. System Options Menu

Item	Options	Default	Help Text	Comment
Continue Booting	N/A	N/A	Select this to boot from the first Boot Option now.	
Boot Manager	N/A	N/A	Select this to boot from one of the available Boot Options. To modify these Boot Options, select Boot Maintenance Manager option in System Options Menu.	Selects Boot Options sub-menu.
Boot Maintenance Manager	N/A	N/A	Select this to modify the available Boot Options, modify Floppy, Hard Drive, CDROM, NIC and BEV boot order. Only one Legacy Hard Drive and one Legacy Floppy Drive in the system can be selected to become the boot drive.	Selects sub-menu.
BIOS Setup Utility	N/A	N/A	Select this to view and configure platform settings.	Opens up the BIOS Setup Utility.
Error Manager	N/A	N/A	Select this to review errors detected this boot.	Selects sub-menu .

11.4 Error Manager

Table 45. Error Manager Menu

Item	Options	Default	Help Text	Comment
Boot Option Menu	N/A	N/A	Use the up or down arrows to select to change option, ENTER to select an option, ESC to exit	Not an active link. This menu provides a list of Boot Options which can be selected for booting.
< Ist Boot Option>	N/A	N/A	N/A	This is the first Boot Option in the boot order. The system by default boots to this Boot Option.
<nth Boot Option>	N/A	N/A	N/A	The available Boot Options vary based on the system configuration. Examples of Boot Options are Legacy CDROM, Hard Drive etc. The number of Boot options and their order can be configured using Boot Maintenance Manager menu.
[EFI Shell]	N/A	N/A	N/A	EFI Shell Boot Option present by default.

11.5 Boot Maintenance Manager

Table 46. Boot Maintenance Manager Menu

Item	Options	Default	Help Text	Comment
Boot Options	N/A	N/A	Modify the system boot order and add/delete Boot Options. System reboot is required after any Boot Option change.	Link to Boot Options menu
Driver Options	N/A	N/A	Modify the EFI driver Boot options	Link to driver options menu
Set Time out Value	N/A	N/A	Modify the automatic boot time-out value.	Link to set time out value
Reset System	N/A	N/A	Reset system	Selecting this option Resets the system

Table 47. Boot Options Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page				Returns to the previous page
Go Back To Main Page	N/A	N/A	Go Back To Main Page	Go back to boot maintenance manager screen
Add Boot Option	N/A	N/A	Add EFI Application or Removable FS as Boot Option. This is for an EFI aware OS contained that supports Simple File protocol.	Link to Add Boot Option screen Adds EFI applications and devices supporting EFI File system application as Boot Options. This option does not support adding any Legacy Boot devices.
Delete Boot Option	N/A	N/A	Valid on next boot	Link to Delete Boot Option screen Deletes added Boot Option.
Change Boot Order	N/A	N/A	Boot the system from a file or a device.	Link to Change Boot Order screen Changes the Boot Order of the Boot Manager Boot Options.
Select Legacy Floppy Order	N/A	N/A	Select Legacy Floppy Order. Only the first floppy in the list becomes the Boot floppy.	Link to Select Legacy Floppy Order screen
Select Legacy Hard Drive Order	N/A	N/A	Select Legacy Hard Drive Order. Only the first Hard Drive in the list becomes the Boot Hard Drive.	Link to Select Legacy Hard Drive screen
Select Legacy CD-ROM	N/A	N/A	Select Legacy CD-ROM Order.	Link to Select Legacy CD-ROM screen
Set Embedded NIC Order	N/A	N/A	Set Embedded NIC Order	Link to Set Embedded NIC Order screen
Set Legacy BEV Order	N/A	N/A	Set Legacy BEV Order	Link to select Set Legacy BEV Order Changes the boot order of [BBS] Specification compliant boot devices supporting BootStrap Entry Vector(BEV)

Table 48. Change Boot Order Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page			Go back to Main Page	Returns to the previous page
Change this option's order (Repeats 'n' times for number of devices)	Varies	varies	Other options change accordingly	Select the Boot Options to define the Boot Order.
Apply Changes				
Discard Changes				

Table 49. Add Boot Option Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page				Returns to the previous page
Go Back To Main Page	N/A	N/A	Go Back To Main Page	Go back to boot maintenance manager screen
String specifying a Boot Option that can be added. (Repeats 'n' times for number of drivers) <string varies>	N/A	N/A		Select this option to add it as a Boot Option. Whether any options appear and what they are varies with system configuration. Once an option is selected, all other options disappear.
Input the description		"-"		Appears once a Boot Option is selected. User can enter a descriptive name string for the Added Boot option.
Input Optional data		"-"		Appears once a Boot Option is selected Optional input data for the corresponding added Boot Option. This data is specific to the added Boot Option.
Apply Changes	N/A	N/A		Selecting this option prompts user to return to the previous menu or go back to the main page. User changes are applied if user returns to the main page

Table 50. Delete Boot Option Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page				Returns to the previous page
Go Back To Main Page	N/A	N/A	Go Back To Main Page	Go back to boot maintenance manager screen
String specifying a Boot Option that can be deleted. (Repeats ‘n’ times for number of drivers) <string varies>	[ ] or [X]	[ ]	String specifying Boot Option. May not be present for some Boot Options. <string varies>	Whether any options appear and what they are varies with system configuration. Toggle the checkbox using <Space bar> or <Enter> key for one or more of the listed Boot Options. When Apply Changes is selected, those Boot Options are removed.
Apply Changes	N/A	N/A		Selecting this option prompts user to return to the previous menu or go back to the main page. User changes are applied if user returns to the main page
Discard Changes	N/A	N/A		Selecting this option prompts user to return to the previous menu or go back to the main page. User changes are discarded if user returns to the main page

Table 51. Select Legacy Floppy Order Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page				Returns to the previous page
Go Back To Main Page	N/A	N/A	Go back to Main Page	Go back to boot maintenance manager screen
Floppy Drive #00 <string - varies>	<varies>	<varies>	Select Floppy Drive #00	First device of type Floppy Disk in the Boot order, (as per [BBS] specification). This drive gets listed in the Boot Manager screen as a user selectable Boot Option. Selecting this Option prompts user to select another Floppy Drive
Floppy Drive #n <string - varies>	<varies>	<varies>	Select Floppy Drive #n	Varies with system configuration.
Apply Changes	N/A	N/A		
Discard Changes	N/A	N/A		

Table 52. Select Legacy Hard Drive Order Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page				Returns to the previous page
Go Back To Main Page	N/A	N/A	Go back to Main Page	Go back to boot maintenance manager screen
Hard Disk Drive #00	<varies>	<varies>	Select Hard Drive #00	First device of type hard disk in the Boot order, (as per [BBS] specification). This drive gets listed in the Boot Manager screen as a user selectable Boot Option. Selecting this option prompts user to select another hard disk
Hard Disk Drive #n <string - varies>	<varies>	<varies>	Select Hard Drive #n	Varies with system configuration.
Apply Changes	N/A	N/A		
Discard Changes	N/A	N/A		

Table 53. Select Legacy CD-ROM Order Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page				Returns to the previous page
Go Back To Main Page	N/A	N/A	Go back to Main Page	Go back to boot maintenance manager screen
ATAPI CDROM Drive #00<string varioes>	<varies>	<varies>	Select ATAPI CDROM Drive #00	
ATAPI CDROM Drive #n<string varies>	<varies>	<varies>	Select ATAPI CDROM Drive #n	
Apply Changes	N/A	N/A		
Discard Changes	N/A	N/A		

Table 54. Set Embedded NIC Order Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page			Go back to Main Page	Returns to the previous page
Go Back To Main Page	N/A	N/A	Go back to Main Page	Go back to boot maintenance manager screen
Embedded NIC Drive#00 <string varies>	<varies>	<varies>	Embedded NIC Drive##00	Varies with system configuration.
Embedded NIC Drive##n <string varies>	<varies>	<varies>	Embedded NIC Drive##n	Varies with system configuration.
Apply Changes	N/A	N/A		
Discard Changes	N/A	N/A		

Table 55. Select Legacy BEV Order Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page			Go back to Main Page	Returns to the previous page
Go Back To Main Page	N/A	N/A	Go back to Main Page	Go back to boot maintenance manager screen
BEV Drive #00 <string varies>	<varies>	<varies>	BEV Drive #00	Varies with system configuration.
BEV Drive #n <string varies>	<varies>	<varies>	BEV Drive #n	Varies with system configuration.
Apply Changes	N/A	N/A		
Discard Changes	N/A	N/A		

Table 56. Driver Options Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page			Go back to Main Page	Returns to the previous page
Go Back To Main Page	N/A	N/A	Go back to Main Page	Go back to boot maintenance manager screen
Add driver option	N/A	N/A	Add .EFI driver as driver Option	Add an EFI driver as a Boot Option. The driver should be compliant to the Extensible Firmware Interface Specification 1.1
Delete driver option	N/A	N/A	Valid on next boot	
Change driver order	N/A	N/A	Valid on next boot	

Table 57. Add Driver Option Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page			Go back to Main Page	Returns to the previous page
Go Back To Main Page			Go Back To Main Page	Go back to Boot Maintenance Manager screen
Add driver option Using File	N/A	N/A	Select a file to add to the driver option list	Link to Add driver option Using File Screen
Add Driver Option Using Handle	N/A	N/A	Select an EFI Handle to add to the driver option list	Link to add driver option Using Handle Screen

Table 58. Add Driver Option Using File Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page				Returns to the previous page
Go Back To Main Page	N/A	N/A	Go Back To Main Page	Go back to boot maintenance manager screen
String specifying a driver option that can be added. (Repeats ‘n’ times for number of drivers) <string varies>	N/A	N/A		Select this option to add it as a driver option. Whether any options appear and what they are varies with system configuration. Once an option is selected, all other options disappear.
Input the description		“-“		Appears once a driver option is selected. Add a descriptive name string for the Added driver option.
Load Option Force Reconnect	[ ] or [X]	[ ]	Load Option Force Reconnect	Appears once a driver option is selected. Toggle the checkbox for forcing a driver to reconnect.
Input Optional data		“-“		Appears once a driver option is selected Optional input data for the added driver option. This data is specific to the driver being added.
Apply Changes	N/A	N/A		Appears once a driver option is selected. Selecting this option prompts user to return to the previous menu or go back to the main page. User changes are applied if user returns to the main page

Table 59. Add Driver Option Using Handle Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page				Returns to the previous page
Go Back To Main Page	N/A	N/A	Go Back To Main Page	Go back to boot maintenance manager screen
String specifying a driver option that can be added. (Repeats 'n' times for number of drivers) <string varies>	N/A	N/A		Select this option to add it as a driver option. Whether any options appear and what they are varies with system configuration. Once an option is selected, all other options disappear.
Input the description		"-"		Appears once a driver option is selected. Add a descriptive name string for the Added driver option.
Load Option Force Reconnect	[ ] or [X]	[ ]	Load Option Force Reconnect	Appears once a driver option is selected.
Input Optional data		"-"		Appears once a driver option is selected. Optional input data for the added driver option. This data is specific to the driver being added.
Apply Changes	N/A	N/A		Appears once a driver option is selected. Selecting this option prompts user to return to the previous menu or go back to the main page. User changes are applied if user returns to the main page

Table 60. Delete Driver Option Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page				Returns to the previous page
Go Back To Main Page	N/A	N/A	Go Back To Main Page	Go back to boot maintenance manager screen
String specifying 1st driver option that can be deleted. (Repeats ‘n’ times for number of drivers) <string varies>	[ ] or [X]	[ ]	String specifying driver option. May not be present for some driver options. <string varies>	Whether any options appear and what they are varies with system configuration. Toggle the checkbox using <Space bar> or <Enter> key for selecting one or more of the listed driver options. When Apply Changes is selected, those driver options are removed.
Apply Changes	N/A	N/A		Appears once a driver option is selected. Selecting this option prompts user to return to the previous menu or go back to the main page. User changes are applied if user returns to the main page
Discard Changes	N/A	N/A		Selecting this option prompts user to return to the previous menu or go back to the main page. User changes are discarded if user returns to the main page

Table 61. Change Driver Order Menu

Item	Options	Default	Help Text	Comment
F2= Previous Page			Go back to Main Page	Returns to the previous page
Go Back To Main Page	N/A	N/A	Go Back To Main Page	Go back to boot maintenance manager screen
Change this option’s order (Repeats ‘n’ times for number of drivers)	Varies	varies	Other options change accordingly	Select the driver Options to define the driver order.
Apply Changes				Appears once a driver option is selected. Selecting this option prompts user to return to the previous menu or go back to the main page. User changes are applied if user returns to the main page
Discard Changes				Selecting this option prompts user to return to the previous menu or go back to the main page. User changes are discarded if user returns to the main page

Table 62. Set Time Out Value Menu

Item	Options	Default	Help Text	Comment
F2 = Previous Page	N/A	N/A		
Go Back to Main Page			Go Back to Main Page	Go back to boot maintenance manager screen
Auto Boot Time -Out	varies	10	Auto boot timeout value in seconds. If a value of 0 is selected, system boots to the default Boot Option without waiting for any user input key. Otherwise system waits for user input for the selected time-out period.	
Apply Changes	N/A	N/A		
Discard Changes	N/A	N/A		

11.6 BIOS Setup Utility

The BIOS setup utility is a text-based utility, which 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 and is entered by selecting system options menu during POST.

The BIOS setup interface consists of a number of pages or screens. Each page contains information or links to other pages. The first page in setup displays a list of general categories as links. These links lead to pages containing the specific category's configuration.

11.6.1 Setup Utility 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 63. BIOS Setup Utility 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 and center columns in the middle of the screen. The left column, the "Setup Item", is the subject of the item. The middle column, the "Option", contains an informational value or choices of the subject. A Setup Item may also be a hyperlink that is used to navigate formsets (pages). When it is a hyperlink, a Setup Item only occupies the “Setup Item” column.
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 includes the meaning and usage of the item, allowable values, effects of the options, etc.
Keyboard Command	The Keyboard Command Bar is located at the bottom right of the screen and

Functional Area	Description
Bar	continuously displays help for keyboard special keys and navigation keys. The keyboard command bar is context-sensitive—it displays keys relevant to current page and mode.
Status Bar	The Status Bar occupies the bottom line of the screen. This area indicates the status of Setup. The status value "NV", indicates that the user has made changes to Setup that have not been saved.

11.6.2 Keyboard Commands

The bottom right portion of the setup screen provides a list of commands that are used to navigate through the setup utility. These commands are displayed at all times.

Each setup menu page contains a number of features. Except those used for informative purposes, each feature is associated with a value field. This field contains user-selectable parameters. Depending on the security option chosen and in effect via password, a menu feature's value can be changeable or not. If a value is non-changeable due to insufficient security privileges (or other reasons), the feature's value field is inaccessible.

Table 64. 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, undo the pick list, and return the focus to the parent menu.
ESC	Exit	The ESC key provides a mechanism for backing out of any field. This key will undo the pressing of the Enter key. 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 any settings. If "Yes" is selected and the Enter key is pressed, 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.
-	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 keyboard, but has the same effect.

Key	Option	Description
F9	Setup Defaults	Pressing F9 causes the following to appear: Load default configuration now? (Y/N) If the "Y" key is pressed, all Setup fields are set to their default values. If the "N" key is pressed, or if the ESC key is pressed, the user is returned to where they were before F9 was pressed without affecting any existing field values
F10	Save and Exit	Pressing F10 causes the following message to appear: Save Configuration changes and exit now? (Y/N) If the "Y" key is pressed, all changes are saved and Setup is exited. If the "N" key 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.

11.6.3 Server Platform Setup

This section lists and describes the pages of a server platform setup. Each table is displayed in setup as a page. The text and values in the Setup Item, Option, and Help columns in Table 65 below are also displayed in their respective setup pages. The Default column indicates the option value applied when setup is reset to default values.

Table 65. Main Menu

Setup Item	Options	Default	Help Text	Comment
Main			Set general system parameters.	Not an active link.
Processor			Examine and set system processor parameters.	Link to processor
Memory			Examine and set system memory parameters	Link to memory
Devices			Examine and set system parameters for built-in devices.	Link to devices
Server Management			Examine and set Server Management parameters	Link to Server Management
Security			Examine and set security options.	Link to Security
Save, Restore and Exit			Save, restore values and/or exit BIOS Setup.	Link to save, restore and exit

Table 66. Time and Date Menu

Setup Item	Options	Default	Help Text	Comment
BIOS Version	N/A	N/A	N/A	Displays the current BIOS version (excluding the build time and date). as per the description in section titled - BIOS Identification String.
System Date	[DD/MM/YYYY]	N/A	Month valid values are 1 to 12. Day valid values are 1 to 31. Year valid values are 1998 to 2099.	Help text depends on the subfield selected (month, day, or year).
System Time	[HH:MM:SS]	N/A	Hours valid values are 0 to 23. Minutes valid values are 0 to 59. Seconds valid values are 0 to 59.	Help text depends on the subfield selected (hours, minutes, econds).
Quiet Boot Enable	Enabled/ Disabled	Enabled	If enabled no messages are displayed on the screen while the system POSTs. System POSTs with the logo displayed.	
POST Error Pause	Enabled/ Disabled	Enabled	If enabled, the system waits for user intervention on critical POST errors. If disabled, the system boots with no intervention, if possible.	

Table 67. Processor Menu

Setup Item	Options	Default	Help Text	Comment
Core Frequency	Current processor Core running frequency.		Frequency at which processors currently run.	Information only
Bus Frequency	Current bus frequency.	Auto	Current frequency of the processor Front Side Bus.	Information only
Processor Retest	Enabled/ Disabled	Disabled	If enabled, retest all processors in the system during the next POST.	Executes only once and then automatically resets to disabled.
Hyper-Threading Enable	Enabled/ Disabled	Enabled	Enables the Hyper-Threading feature, takes effect after reboot.	
Boot Processor Number	Processor #<the BSP number)		Number of the processor that is designated by the firmware to boot this system.	Information only
Processor #<processor number> Information			Processor Detailed Information.	Information only. Link to processor #<processor number> screen (one per processor supported by the platform).

Table 68. Processor #n Information Menu

Setup Item	Options	Default	Help Text	Comment
Processor Family	<processor family string>		Identifies family or generation of the processor.	Information only
Maximum Frequency	<processor max frequency in MHz or GHz>		Maximum frequency the processor core supports.	Information only
Cache Size	<processor cache size in KBs or MBs>		Size of the processor cache.	Information only
CPUID Register			CPUID register value identifies details about the processor model.	Information only
Thread n Status	<Boot Thread/Application Thread/Not Installed/ Disabled>		A thread could have one of the following statuses: “Boot Thread” – machine has booted using this thread; “Application Thread” – the thread is available to be used by the OS; “Not Installed” – processor or thread is not installed; “Disabled” – the thread is disabled.	Information only
Thread n Health	<Healthy /Performance Restricted/Functionality Restricted/Failed/Not Installed>		A thread could be one of the following: “Healthy", “Performance Restricted”, “Functionality Restricted”, “Failed” or “Not Installed”.	Information only

Table 69. Memory Menu

Setup Item	Options	Default	Help Text	Comment
Total Memory	<the amount of memory in MB or GB>		Total good memory from all slots available for use by the system.	Information only
Effective Memory	<the amount of memory in MB or GB available to the OS>		Amount of memory that can be used by Operating System. Effective memory may be less than total memory if some memory is used for redundancy.	Information only
Memory boards Installed	<A,B,C,D>		Memory boards plugged into the system.	Information only
Current Configuration	< Maximum Compatibility/ Maximum Performance/Mirror/ RAID >		Current memory configuration for the system.	Information only
Configure Memory RAS and Performance			Select this page to view and configure memory RAS (Reliability Accessibility and Serviceability) and performance features.	Link to configure system RAS and performance.

Setup Item	Options	Default	Help Text	Comment
View and Configure memory board #<board number>			Select this page to view and configure memory board features.	Link to memory board #<board number>, one per memory board supported by the platform.

Table 70. Configure System RAS and Performance Menu

Setup Item	Option	Default	Help Text	Comment
Hardware Memory Test	Enabled/ Disabled	Enabled	If enabled, the memory is tested using hardware based engines on each board.	
Patrol Scrub	Enabled/ Disabled	Enabled	Enable hardware patrol scrub to clean correctable errors.	
Retest All System Memory	Enabled/ Disabled	Disabled	If enabled, retests all memory in the system (including disabled DIMMs) and enables memory which passes the test. This option resets to Disabled after the test has run.	
Sparing Threshold	1-15	15	Set the number of correctable errors that can be logged in a period before sparing occurs. Period is 12 or 16 days depending on DDR Technology.	
RAID Upgrade Gap	Disabled, 512MB, 1024MB, 1536MB, 2048MB, 2560MB, 3072MB, 3584MB, 4096MB	Disabled	Size of reserved gap on each memory board for RAID memory capacity addition.	
Desired Memory Configuration	Max Performance/ Max Compatibility/ Mirror RAID	Max Performance	Select a new memory configuration. Then select view configuration details to see the configuration.	
View Configuration Details	N/A	N/A	Select this to view memory configuration details page.	Link to view memory configuration details
Set Memory Hotplug in SRAT table	Yes/No	Yes	This enables or disables hot-pluggable flag in Resource Affinity Table for memory region above 4GB. Setting to No may disable memory capcity add or remove under some OS.	

Table 71. View Memory Configure Details Menu

Setup Item	Option	Default	Help Text	Comment
Configuration	<Max Performance/ Max Compatibility/ Mirror/RAID>		**Help Text for Max Performance** This 4-way interleave configuration provides the maximum performance. To get maximum performance f boards of same size should be installed. (A:B:C:D) **Help Text for Max Compatibility** This compatibility configuration is 1-way interleave. It allows the use of any number of memory boards. Each may be of different sizes. (A),(B),(C),(D) **Help Text for Mirror** Boards (A)(B) and (C)(D) are mirrored. **Help Text for RAID** RAID configuration requires four boards of same size to be installed. Data is stored on three boards while the fourth board contains redundancy information.	Information only. <As per configuration selected on previous page>
Max Effective Size	<Max possible size of memory in MB>		Maximum effective memory size results when no spares are configured. The actual effective size is calculated on the next boot.	Information only
Min Effective Size	<Min possible size of memory in MB>		Minimum effective memory size results when the largest DIMMs are used as spare (Auto spare configuration). The actual effective size is calculated on the next boot.	Information only
Configuration Capabilities			Characteristics of the selected configuration.	Title only
Configuration Possible	<Yes/ No>		Indicates whether the configuration selected is possible with the current installed memory.	Information only
Sparing	<Yes/ No>		Indicates whether the configuration supports sparing.	Information only
Hot Replace	<Yes/ No>		Indicates whether configuration allows memory to be replaced while system is running.	Information only
Hot Add	<Yes/ No>		Indicates whether the configuration allows memory to be added while the system	Information only

Setup Item	Option	Default	Help Text	Comment
			is running.	
Board Interleave	<1-Way/2-Way/4-Way/Mixed>		This is the board interleave for the chosen configuration. In mixed interleave, the BIOS configures the best possible interleave for each memory range.	Information only

Table 72. Memory Board #n Menu

Setup Item	Option	Default	Help Text	Comment
Board Status	Not Installed/ Healthy/ Using Spare/ Disabled		Indicates board status. Possible values are: Not Installed, Healthy, Using Spare, or Disabled.	Information only
Retest Board Memory	Enabled/ Disabled	Disabled	If enabled, re-test all DIMMs on the current board and re-enable the DIMMs that pass the test. This option is reset to 'Disabled' after the test has been run.	
Reserve rank for Spare	Enable/Disable	Disabled	If enabled, the BIOS sets aside the largest memory rank to serve as spare. When correctable errors on a bad rank surpasses the sparing threshold, it is replaced by a spare rank.	
DIMM Labels Menu (Table 73)	Not-Installed/ Installed/ Installed/partial/ Failed		Label is the DIMM slot board label. DIMMs must be populated in pairs and can occupy 1 rank (single sided pair) or 2 rank (double sided pair). DIMM state may be: Installed, Not-Installed, Installed/Partial or Failed Memory slot status of: "Installed" – memory is installed and healthy. "Not Installed" – the slot is empty. "Installed/Partial" – memory is installed but only part of it is used. "Failed" – memory has been reported as failed.	Information only

Table 73. DIMM Labels Menu

Label	Rank	Size	Status
DIMM1A	1/2	Size in MB or GB	Not-Installed/Installed/Installed/partial/Failed
DIMM1B	1/2	Size in MB or GB	Not-Installed/Installed/Installed/partial/Failed
DIMM2A	3/4	Size in MB or GB	Not-Installed/Installed/Installed/partial/Failed
DIMM2B	3/4	Size in MB or GB	Not-Installed/Installed/Installed/partial/Failed

Table 74. Devices Menu

Setup Item	Option	Default	Help Text	Comment
IDE Controller			Examine and set IDE controller parameters.	Link to setup utility\devices\IDE Controller
Mass Storage			Examine and set mass storage controller's parameters.	Link to setup utility\devices\Mass Storage
LAN			Examine and set Local Area Network (LAN) parameters.	Link to setup utility\devices\LAN
Video			Examine and set Video parameters.	Link to setup utility\devices\Video
USB			Examine and set USB controller parameters.	Link to setup utility\devices\USB
Serial Ports			Examine and set Serial Ports parameters.	Link to setup utility\devices\Serial Ports
PCI			Examine and set PCI system parameters.	Link to setup utility\devices\PCI

Table 75. IDE Controller Menu

Setup Item	Option	Default	Help Text	Comment
Enable SATA Controller	Enabled/ Disabled	Enabled	Enables and disables Serial ATA controller - all channels. If disabled, the Serial ATA controller is not visible to the OS	
Primary Master	<the IDE device name string>			Information only

Table 76. Mass Storage Menu

Setup Item	Option	Default	Help Text	Comment
Enable On-board SCSI	Enabled/ Disabled	Enabled	If Disabled, the embedded SCSI device is turned off and device is inaccessible to the OS.	Grayed out if ROMB is enabled,
RAID Activation Key	Installed/Not Installed		If Intel® RAID Activation Key is installed, the Intel® RAID-on-Motherboard (ROMB) option is activated. The onboard SCSI option becomes unavailable and cannot be changed while the Intel® RAID Activation Key is installed. WARNING: BACK UP EXISTING DATA AND DELTETE EXISTING ARRAYS (IF ANY) BEFORE UPGRADING TO ROMB. ROMB Configuration overwrites existing data on disks. Intel® RAID-on-MotherBoard solution requires the use of the Intel® RAID Activation Key and a DDR2 DIMM. Refer to product documentation for RAID configuration details.	Information only. Reports the ROMB Intel® RAID Activation Key presence status.

Table 77. LAN Menu

Setup Item	Option	Default	Help Text	Comment
Enable On-board NIC	Enabled/ Disabled	Enabled	If disabled, both channels of the embedded LAN are turned off and the device is inaccessible to the OS.	
Enable On-board NIC ROM	Enabled/ Disabled	Enabled	If enabled, the Option ROM for the Onboard LAN is executed.	
NIC 1 MAC Address	<12 hex digits of the MAC address>	N/A	Media Access Control (MAC) of the LAN controller on this system over which Server Management tasks are performed.	Information only
NIC 2 MAC Address	<12 hex digits of the MAC address>	N/A	Media Access Control (MAC) of the LAN controller on this system over which Server Management tasks are performed.	Information only

Table 78. Video Menu

Option	Option	Default	Help Text	Comment
Enable On-board Video	Enabled/ Disabled	Enabled	If disabled, the embedded video is turned off and the device is inaccessible to the OS.	

Table 79. USB Menu

Setup Item	Option	Default	Help Text	Comment
USB Controller Enable	Enabled/ Disabled	Enabled	If disabled, the USB controller is turned off and inaccessible by the OS.	
USB 2.0 Controller	Enabled/ Disabled	Enabled	Enables/Disables USB 2.0 Controller	

Table 80. Serial Ports Menu

Setup Item	Option	Default	Help Text	Comment
COM 1 Enable	Enabled/ Disabled	Enabled	Enables or disables COM1 port.	
Address	3F8/2F8/3E8/ 2E8	3F8	Selects the base I/O address for COM1.	
IRQ	3/4	4	Selects the Interrupt Request line for COM1.	

Table 81. PCI Menu

Setup Item	Option	Default	Help Text	Comment
Enable Slot 1 ROM	Enabled/ Disabled	Enabled	Enables/Disables Option ROM scan of the device in PCI slot 1.	
Enable Slot 2 ROM	Enabled/ Disabled	Enabled	Enables/Disables Option ROM scan of the device in PCI slot 2.	
Enable Slot 3 ROM	Enabled/ Disabled	Enabled	Enables/Disables Option ROM scan of the device in PCI slot 3.	
Enable Slot 4 ROM	Enabled/ Disabled	Enabled	Enables/Disables Option ROM scan of the device in PCI slot 4.	
Enable Slot 5 ROM	Enabled/ Disabled	Enabled	Enables/Disables Option ROM scan of the	

Setup Item	Option	Default	Help Text	Comment
			device in PCI slot 5.	
Enable Slot 6 ROM	Enabled/ Disabled	Enabled	Enables/Disables Option ROM scan of the device in PCI slot 6.	
Enable Slot 7 ROM	Enabled/ Disabled	Enabled	Enables/Disables Option ROM scan of the device in PCI slot 7.	
Enable FC Card ROM	Enabled/ Disabled	Enabled	Enable/Disable posting a 16-bit Legacy Option-ROM from plug-in Fiber Channel Card.	

Table 82. Server Management Menu

Setup Item	Option	Default	Help Text	Comment
Console Redirection	N/A	N/A	Examine and set console redirection parameters.	Link to Console Redirection
FRU Information	N/A	N/A	Examine Field Replaceable Units (FRU) parameters.	Link to FRU Information
LAN Management	N/A	N/A	Examine and set System LAN Management options.	Link to LAN Management
SEL Logging	N/A	N/A	Examine and set System Event Log (SEL) options.	Link to SEL Logging
FRB Information	N/A	N/A	Examine and set Fault Resilient Boot (FRB) options.	Link to FRB Information
WOL Resume from S5	Disabled/ Enabled	Enabled	This enables or disables system wake from S5 on Wake On LAN (WOL). Note that PCI/PCI-e LAN cards must support PME/ EXP_WAKE assertion on WOL.	None

Table 83. Console Redirection Menu

Setup Item	Option	Default	Help Text	Comment
Com1 Console Redirection			Examine and set COM1 console redirection parameters.	Link to COM1 Console Redirection

Table 84. COM1 Console Redirection Menu

Setup Item	Option	Default	Help Text	Comment
BIOS Console Redirection	Enabled/ Disabled	Disabled	Enables performing Server Management tasks over the serial port.	
Flow Control	None RTS/CTS XON/XOFF CTS/RTS + CD	None	Selects serial port communication protocol handshaking type.	
Baud Rate	9600/19.2K/38.4K/57.6K/115.2K	19.2K	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.	
Terminal Type	VT100/ VT100+/ VT-UTF8/ PC-ANSI	VT100+	VT100/VT100+ selection only works with English language. VT-UTF8 uses Unicode. PC-ANSI is the standard PC-type terminal.	

Table 85. FRU Information Menu

Setup Item	Option	Default	Help Text	Comment
Board Part Number	<string from the FRU>			Information only
Board Serial Number	<string from the FRU>			Information only
System Part Number	<string from the FRU>			Information only
System Serial Number	<string from the FRU>			Information only
Chassis Part Number	<string from the FRU>			Information only
Chassis Serial Number	<string from the FRU>			Information only
BMC Device ID	<string from the BMC>		Device identification number of the Baseboard Management Controller	Information only

Setup Item	Option	Default	Help Text	Comment
BMC Firmware Revision	<string from the BMC>			Information only
BMC Device Revision	<string from the BMC			Information only
PIA Revision	<string from the BMC>			Information only
SDR Revision	<string from the BMC>			Information only
Hot Swap Controller	<string from the Hot Swap Controller>		Revision of the Hot Swap Back Plane (HSBP) controller firmware.	Information only

Table 86. LAN Management Menu

Setup Item	Option	Default	Help Text	Comment
LAN Controller 1:	N/A	N/A	N/A	Title for next items
Static IP Enable	Enabled/ Disabled	<loaded from BMC>	Allows Host and Router IP addresses to be manually specified. If disabled, the IP addresses are automatically assigned by the system.	
Host IP Address	<000.000.000.000 format string>	<loaded from BMC>	IP address of the host system.	If Static IP Enable option is enabled, then the IP Address can be manually specified. The user is prompted for the IP address data.
Router IP Address	<000.000.000.000 format string>	<loaded from BMC>	IP address of the router system.	If Static IP Enable option is enabled, then the IP Address can be manually specified. The User is prompted for the IP address data.
NIC 1 MAC Address	<string from the BMC>	<loaded from BMC>	Media Access Control address of LAN device.	Media Access Control (MAC) of the LAN controller on this system over which Server Management tasks are performed.

Table 87. SEL Menu

Setup Item	Option	Default	Help Text	Comment
Clear Log	Enabled/ Disabled	Disabled	Clears the System Event Log. All entries are lost. Space for more log entries is reclaimed.	This option executes as soon as it is selected and then resets to disabled.

Table 88. FRB Information Menu

Setup Item	Option	Default	Help Text	Comment
Processor #<processor number> Information			Processor Detailed Information.	Link to #<processor number> Information, one per processor supported by the platform
FRB-2 Enable	Enabled/ Disabled	Enabled	If enabled, the BMC resets the system if the BIOS does not complete the Power On Self Test before the FRB-2 timer expires.	
OS WD Timer Enable	Enabled/ Disabled	Disabled	If enabled, the timer starts when the system begins to boot an Operating System. If the timer expires before the Operating System boot completes, the system is reset by the BMC.	
OS WD Timer	5 minutes/ 10 minutes/ 15 minutes/ 20 minutes	10 minutes	This sets the time that the system has to boot an Operating System.	This option is grayed out if the “OS WD Timer Enable option” is not selected.

Table 89. Security Menu

Setup Item	Option	Default	Help Text	Comment
Administrator Password is	Installed/Not Installed	Not Installed	Indicates the status of administrator password.	Information only, Disabled if the password is blank, Active otherwise
Set Administrator Password			The administrator password controls access to platform configuration.	The password is not displayed
User Password	Installed/Not Installed	Not Installed	Indicates the status of user password.	Information only, Disabled if the password is blank, Active otherwise
Set User Password			The user password controls access to the system at boot.	
Password on Boot	Enabled/ Disabled	Disabled	If enabled, password entry is required before boot.	

Table 90. Save, Restore and Exit Menu

Setup Item	Option	Default	Help Text	Comment
Save Changes and Exit			Apply current values and exit the BIOS Setup.	User is prompted for confirmation only if any of the setup fields were modified.
Discard Changes and Exit			Ignore changes made to values and exit the BIOS Setup.	User is prompted for confirmation only if any of the setup fields were modified.
Save Changes			Apply current values and continue the BIOS Setup.	User is prompted for confirmation only if any of the setup fields were modified.
Discard Changes			Undo changes made to values and continue the BIOS Setup.	User is prompted for confirmation only if any of the setup fields were modified.
Restore Defaults			Restore the default BIOS Setup values.	User is prompted for confirmation. The BIOS loads the defaults on the next reboot.
Save User Default Values			Save current values so they can be restored later.	
Restore User Default Values			Restore previously saved user default.	User is prompted for confirmation.

12. Error Handling

12.1 LEDs

12.1.1 POST Progress LEDs

The BIOS provides the current stage of the POST process via a block of eight LEDs. The LEDs are shown in Table 91.

Table 91. POST Progress LED Location and Example

LED Reference Designator	Bit	Example: Initialize Memory	
DS7D2	7 (MSB)		0x27
DS7D3	6		
DS7D4	5	On	
DS7D5	4		
DS7D6	3		
DS7E1	2	On	
DS7E2	1	On	
DS7E3	0 (LSB)	On	

Table 92. POST Progress LED Codes

Code	Description
Host Processor:	
0x10	Power-on initialization of the host processor (Boot Strap Processor)
0x11	Host processor cache initialization, including Application Processor (AP)
0x12	Starting AP initialization
0x13	SMM initialization
Chipset:	
0x21	Initializing a chipset component
Memory:	
0x22	Reading configuration data from memory (SPD on DIMM)
0x23	Detecting presence of memory
0x24	Programming timing parameters in the memory controller
0x25	Configuring memory parameters in the memory controller
0x26	Optimizing memory controller settings
0x27	Initializing memory, such as ECC init
0x28	Testing memory
PCI Bus:	
0x50	Enumerating PCI busses
0x51	Allocating resources to PCI buses
0x52	PCI Hot-Plug controller initialization

Code	Description
0x53-0x57	Reserved for PCI Bus
USB:	
0x58	Resetting USB bus
0x59	Reserved for USB devices
SATA:	
0x5A	Resetting SATA bus and all devices
0x5B	Reserved for ATA
SMBUS:	
0x5C	Resetting SMBUS
0x5D	Reserved for SMBUS
Local Console:	
0x70	Resetting the video controller (VGA)
0x71	Disabling the video controller (VGA)
0x72	Enabling the video controller (VGA)
Remote Console:	
0x78	Resetting the console controller
0x79	Disabling the console controller
0x7A	Enabling the console controller
Keyboard:	
0x90	Resetting the keyboard
0x91	Disabling the keyboard
0x92	Detecting the presence of the keyboard
0x93	Enabling the keyboard
0x94	Clearing keyboard input buffer
0x95	Instructing keyboard controller to run Self Test
Mouse:	
0x98	Resetting the mouse
0x99	Detecting the mouse
0x9A	Detecting the presence of mouse
0x9B	Enabling the mouse
Fixed Media:	
0xB0	Resetting fixed media device
0xB1	Disabling fixed media device
0xB2	Detecting presence of a fixed media device
0xB3	Enabling/configuring a fixed media device
Removable Media:	
0xB8	Resetting removable media device
0xB9	Disabling removable media device
0xBA	Detecting presence of a removable media device
0xBC	Enabling/configuring a removable media device
BDS:	
0xDy	Trying boot selection y (where y = 0 to F)
PEI Core:	
0xE0	Started dispatching early initialization modules (PEIM)

Code	Description
0xE2	Initial memory found, configured, and installed correctly
0xE, 0xE3	Reserved for initialization module use (PEIM)
DXE Core:	
0xE4	Entered EFI driver execution phase (DXE)
0xE5	Started dispatching drivers
0xE6	Started connecting drivers
DXE Drivers:	
0xE7	Waiting for user input
0xE8	Checking password
0xE9	Entering the BIOS setup
0xEA	Flash update
0xEE	Calling Int 19. One beep unless silent boot is enabled.
0xEF	Unrecoverable Boot failure/S3 resume failure
Runtime Phase/EFI OS Boot:	
0xF4	Entering Sleep state
0xF5	Exiting Sleep state
0xF8	OS has requested EFI to close boot services
0xF9	OS has switched to virtual address mode
0xFA	OS has requested the system to reset
PEIM/Recovery:	
0x30	Crisis recovery has been initiated because of a user request
0x31	Crisis recovery has been initiated by software (corrupt flash)
0x34	Loading crisis recovery capsule
0x35	Handing off control to the crisis recovery capsule
0x3F	Unable to complete crisis recovery.

12.1.2 CPU Diagnostic LEDs

The BMC provides one amber LED per processor. The LEDs are turned on when a CPU has an error.

Table 93. Processor Diagnostic LED Locations

LED Reference Designator	Processor
DS5C1	1
DS5C2	2
DS5C3	3
DS5C4	4

12.2 Beeps

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 POST progress LEDs.

Table 94. Beep Codes

Beeps	Error Message	Description
1	Fatal error	System halted because of an unspecified fatal error that was detected.
2	Processor error	System halted because a fatal error related to a processor was detected.
3	Memory error	System halted because a fatal error related to the memory was detected.
4	Motherboard error	System halted because a fatal error related to the system motherboard hardware was detected.
1-5-1-1		FRB3 failure (processor failure)
1-5-2-1		CPU: empty slot
1-5-2-2		CPU: no processors
1-5-2-3		CPU: configuration error (example VID mismatch)
1-5-2-4		CPU: configuration error (example BSEL mismatch)
1-5-4-2		Power fault: DC power unexpectedly lost (power control failure)
1-5-4-3		Chipset control failure
1-5-4-4		Power control fault (Usually a VRM is not installed.)

12.2.1 BIOS Recovery Beep Codes

Table 95. BIOS Recovery Beep Codes

Beeps	Error Message	POST Progress Code	Description
1 beep	Recovery Started	E9h	Start of recovery process
2 beeps	Recovery Boot Error	Flashing series of POST codes: EFh, FAh, FBh, F4h, FCh, FDh, FFh	Unable to boot to floppy, disk drive, or optical drive. Recovery process retries.
A series of long low-pitched single beeps	Recovery Failed	FDh	Unable to process valid the BIOS recovery images. The BIOS already passed control to operating system and flash utility.
4 long high-pitched beeps	Recovery Complete	FFh	The BIOS recovery succeeded, ready for power-down, reboot.

12.3 POST Messages

The following table describes error codes, the associated error message, and the system handling of the error. If the Warn is “Yes”, the error is of low consequence and has little impact on system functionality. If the Log is “Yes”, the event is stored in the system error log (SEL). If the Display is “Yes”, the error message is displayed to the console(s). If the view is “Yes”, the user must view the error prior to booting. If the Boot is “No”, the system does not boot with this error. If the Halt is “Yes”, the system does not allow any further action.

Table 96. POST Messages

Code	Message	Severity	Response
0012	CMOS Date/Time not set	Major	Pause
004C	Keyboard/Interface error	Major	Pause
5220	Configuration cleared by Jumper	Major	Pause
5221	Passwords cleared by Jumper	Major	Pause
5222	Configuration cleared by BMC	Major	Pause
5223	Configuration default loaded	Major	Pause
0048	Password check failed	Major	Halt
0141	PCI Resource Conflict	Major	Pause
0146	Insufficient Memory to Shadow PCI ROM	Major	Pause
8110	Processor 01 Internal error (IERR)	Minor	Warning
8111	Processor 02 Internal Error (IERR)	Minor	Warning
8112	Processor 03 Internal Error (IERR)	Minor	Warning
8113	Processor 04 Internal Error (IERR)	Minor	Warning
8120	Processor 01 Thermal Trip Error	Minor	Warning
8121	Processor 02 Thermal Trip Error	Minor	Warning
8122	Processor 03 Thermal Trip Error	Minor	Warning
8123	Processor 04 Thermal Trip Error	Minor	Warning
8130	Processor 01 Disabled	Minor	Warning
8131	Processor 02 Disabled	Minor	Warning
8132	Processor 03 Disabled	Minor	Warning
8133	Processor 04 Disabled	Minor	Warning
8140	Processor 01 Failed FRB-3 Timer	Minor	Warning
8141	Processor 02 Failed FRB-3 Timer	Minor	Warning
8142	Processor 03 Failed FRB-3 Timer	Minor	Warning
8143	Processor 04 Failed FRB-3 Timer	Minor	Warning
8160	Processor 01 unable to apply Microcode update	Major	Pause
8161	Processor 02 unable to apply Microcode update	Major	Pause
8162	Processor 03 unable to apply Microcode update	Major	Pause
8163	Processor 04 unable to apply Microcode update	Major	Pause
8180	BIOS does not support the current stepping for processor 1	Major	Pause
8181	BIOS does not support the current stepping for processor 2	Major	Pause
8182	BIOS does not support the current stepping for processor 3	Major	Pause
8183	BIOS does not support the current stepping for processor 4	Major	Pause
8190	Watchdog Timer Failed on Last Boot	Minor	Warning

Code	Message	Severity	Response
8198	OS boot watchdog timer failure	Major	Pause
0192	L3 cache size mismatch	Major	Pause
0193	CPUID, Processor stepping are different	Major	Pause
0194	CPUID, Processor family are different	Major	Pause
0195	Front side bus mismatch.	Major	Pause
0196	CPUID, Processor Model are different	Major	Pause
81A0	Intel® Management Module firmware and FRUSDR update required.	Major	Pause
0197	Processor speeds mismatched	Major	Pause
8300	Baseboard Management Controller failed Self Test	Major	Pause
8306	Front Panel Controller Locked	Minor	Warning
8305	Hotswap Controller Failed	Major	Pause
84F2	BaseBoard Management Controller failed to respond	Major	Pause
84F3	BaseBoard Management Controller in Update Mode	Major	Pause
84F4	Sensor Data Record Empty	Major	Pause
84FF	System Event Log Full	Minor	Warning
8500	Board: A, DIMM: 1A Memory bad or missing	Major	Pause
8501	Board: A, DIMM: 1B Memory bad or missing	Major	Pause
8502	Board: A, DIMM: 2A Memory bad or missing	Major	Pause
8503	Board: A, DIMM: 2B Memory bad or missing	Major	Pause
8508	Board: B, DIMM: 1A Memory bad or missing	Major	Pause
8509	Board: B, DIMM: 1B Memory bad or missing	Major	Pause
850A	Board: B, DIMM: 2A Memory bad or missing	Major	Pause
850B	Board: B, DIMM: 2B Memory bad or missing	Major	Pause
8510	Board: C, DIMM: 1A Memory bad or missing	Major	Pause
8511	Board: C, DIMM: 1B Memory bad or missing	Major	Pause
8512	Board: C, DIMM: 2A Memory bad or missing	Major	Pause
8513	Board: C, DIMM: 2B Memory bad or missing	Major	Pause
8518	Board: D, DIMM: 1A Memory bad or missing	Major	Pause
8519	Board: D, DIMM: 1B Memory bad or missing	Major	Pause
851A	Board: D, DIMM: 2A Memory bad or missing	Major	Pause
851B	Board: D, DIMM: 2B Memory bad or missing	Major	Pause
8520	Board: A, DIMM: 1A Memory not configured	Major	Pause
8521	Board: A, DIMM: 1B Memory not configured	Major	Pause
8522	Board: A, DIMM: 2A Memory not configured	Major	Pause
8523	Board: A, DIMM: 2B Memory not configured	Major	Pause
8528	Board: B, DIMM: 1A Memory not configured	Major	Pause
8529	Board: B, DIMM: 1B Memory not configured	Major	Pause
852A	Board: B, DIMM: 2A Memory not configured	Major	Pause
852B	Board: B, DIMM: 2B Memory not configured	Major	Pause
8530	Board: C, DIMM: 1A Memory not configured	Major	Pause
8531	Board: C, DIMM: 1B Memory not configured	Major	Pause
8532	Board: C, DIMM: 2A Memory not configured	Major	Pause
8533	Board: C, DIMM: 2B Memory not configured	Major	Pause
8538	Board: D, DIMM: 1A Memory not configured	Major	Pause

Code	Message	Severity	Response
8539	Board: D, DIMM: 1B Memory not configured	Major	Pause
853A	Board: D, DIMM: 2A Memory not configured	Major	Pause
853B	Board: D, DIMM: 2B Memory not configured	Major	Pause
8540	Board: A, DIMM: 1A Memory disabled	Major	Pause
8541	Board: A, DIMM: 1B Memory disabled	Major	Pause
8542	Board: A, DIMM: 2A Memory disabled	Major	Pause
8543	Board: A, DIMM: 2B Memory disabled	Major	Pause
8548	Board: B, DIMM: 1A Memory disabled	Major	Pause
8549	Board: B, DIMM: 1B Memory disabled	Major	Pause
854A	Board: B, DIMM: 2A Memory disabled	Major	Pause
854B	Board: B, DIMM: 2B Memory disabled	Major	Pause
8550	Board: C, DIMM: 1A Memory disabled	Major	Pause
8551	Board: C, DIMM: 1B Memory disabled	Major	Pause
8552	Board: C, DIMM: 2A Memory disabled	Major	Pause
8553	Board: C, DIMM: 2B Memory disabled	Major	Pause
8558	Board: D, DIMM: 1A Memory disabled	Major	Pause
8559	Board: D, DIMM: 1B Memory disabled	Major	Pause
855A	Board: D, DIMM: 2A Memory disabled	Major	Pause
855B	Board: D, DIMM: 2B Memory disabled	Major	Pause
8560	Board: A, DIMM: 1A Memory mismatch	Major	Pause
8561	Board: A, DIMM: 1B Memory mismatch	Major	Pause
8562	Board: A, DIMM: 2A Memory mismatch	Major	Pause
8563	Board: A, DIMM: 2B Memory mismatch	Major	Pause
8568	Board: B, DIMM: 1A Memory mismatch	Major	Pause
8569	Board: B, DIMM: 1B Memory mismatch	Major	Pause
856A	Board: B, DIMM: 2A Memory mismatch	Major	Pause
856B	Board: B, DIMM: 2B Memory mismatch	Major	Pause
8570	Board: C, DIMM: 1A Memory mismatch	Major	Pause
8571	Board: C, DIMM: 1B Memory mismatch	Major	Pause
8572	Board: C, DIMM: 2A Memory mismatch	Major	Pause
8573	Board: C, DIMM: 2B Memory mismatch	Major	Pause
8578	Board: D, DIMM: 1A Memory mismatch	Major	Pause
8579	Board: D, DIMM: 1B Memory mismatch	Major	Pause
857A	Board: D, DIMM: 2A Memory mismatch	Major	Pause
857B	Board: D, DIMM: 2B Memory mismatch	Major	Pause
8580	Board: A, DIMM: 1A Memory correctable ECC error	Major	Pause
8581	Board: A, DIMM: 1B Memory correctable ECC error	Major	Pause
8582	Board: A, DIMM: 2A Memory correctable ECC error	Major	Pause
8583	Board: A, DIMM: 2B Memory correctable ECC error	Major	Pause
8588	Board: B, DIMM: 1A Memory correctable ECC error	Major	Pause
8589	Board: B, DIMM: 1B Memory correctable ECC error	Major	Pause
858A	Board: B, DIMM: 2A Memory correctable ECC error	Major	Pause
858B	Board: B, DIMM: 2B Memory correctable ECC error	Major	Pause
8590	Board: C, DIMM: 1A Memory correctable ECC error	Major	Pause

Code	Message	Severity	Response
8591	Board: C, DIMM: 1B Memory correctable ECC error	Major	Pause
8592	Board: C, DIMM: 2A Memory correctable ECC error	Major	Pause
8593	Board: C, DIMM: 2B Memory correctable ECC error	Major	Pause
8598	Board: D, DIMM: 1A Memory correctable ECC error	Major	Pause
8599	Board: D, DIMM: 1B Memory correctable ECC error	Major	Pause
859A	Board: D, DIMM: 2A Memory correctable ECC error	Major	Pause
859B	Board: D, DIMM: 2B Memory correctable ECC error	Major	Pause
85A0	Board: A, DIMM: 1A Memory uncorrectable ECC error	Major	Pause
85A1	Board: A, DIMM: 1B Memory uncorrectable ECC error	Major	Pause
85A2	Board: A, DIMM: 2A Memory uncorrectable ECC error	Major	Pause
85A3	Board: A, DIMM: 2B Memory uncorrectable ECC error	Major	Pause
85A8	Board: B, DIMM: 1A Memory uncorrectable ECC error	Major	Pause
85A9	Board: B, DIMM: 1B Memory uncorrectable ECC error	Major	Pause
85AA	Board: B, DIMM: 2A Memory uncorrectable ECC error	Major	Pause
85AB	Board: B, DIMM: 2B Memory uncorrectable ECC error	Major	Pause
85B0	Board: C, DIMM: 1A Memory uncorrectable ECC error	Major	Pause
85B1	Board: C, DIMM: 1B Memory uncorrectable ECC error	Major	Pause
85B2	Board: C, DIMM: 2A Memory uncorrectable ECC error	Major	Pause
85B3	Board: C, DIMM: 2B Memory uncorrectable ECC error	Major	Pause
85B8	Board: D, DIMM: 1A Memory uncorrectable ECC error	Major	Pause
85B9	Board: D, DIMM: 1B Memory uncorrectable ECC error	Major	Pause
85BA	Board: D, DIMM: 2A Memory uncorrectable ECC error	Major	Pause
85BB	Board: D, DIMM: 2B Memory uncorrectable ECC error	Major	Pause
85C0	Board: A, DIMM: 1A Memory invalid speed	Major	Pause
85C1	Board: A, DIMM: 1B Memory invalid speed	Major	Pause
85C2	Board: A, DIMM: 2A Memory invalid speed	Major	Pause
85C3	Board: A, DIMM: 2B Memory invalid speed	Major	Pause
85C8	Board: B, DIMM: 1A Memory invalid speed	Major	Pause
85C9	Board: B, DIMM: 1B Memory invalid speed	Major	Pause
85CA	Board: B, DIMM: 2A Memory invalid speed	Major	Pause
85CB	Board: B, DIMM: 2B Memory invalid speed	Major	Pause
85D0	Board: C, DIMM: 1A Memory invalid speed	Major	Pause
85D1	Board: C, DIMM: 1B Memory invalid speed	Major	Pause
85D2	Board: C, DIMM: 2A Memory invalid speed	Major	Pause
85D3	Board: C, DIMM: 2B Memory invalid speed	Major	Pause
85D8	Board: D, DIMM: 1A Memory invalid speed	Major	Pause
85D9	Board: D, DIMM: 1B Memory invalid speed	Major	Pause
85DA	Board: D, DIMM: 2A Memory invalid speed	Major	Pause
85DB	Board: D, DIMM: 2B Memory invalid speed	Major	Pause
85E0	Board: A Memory bad or missing	Major	Pause
85E8	Board: B Memory bad or missing	Major	Pause
85F0	Board: C Memory bad or missing	Major	Pause
85F8	Board: D Memory bad or missing	Major	Pause
85E1	Board: A Memory not configured.	Major	Pause

Code	Message	Severity	Response
85E9	Board: B Memory not configured	Major	Pause
85F1	Board: C Memory not configured	Major	Pause
85F9	Board: D Memory not configured	Major	Pause
85FC	System Memory bad or missing	Major	Pause
85FD	System Memory not configured	Major	Pause

Reference Documents

Advanced Configuration and Power Interface Specification, Revision 1.0b.

Intelligent Chassis Management Bus (ICMB) Specification, Version 1.0, Rev 1.20.

Intelligent Platform Management Bus Communications Protocol Specification, Version 1.0.

Intelligent Platform Management Interface Specification, Version 2.0.

Microsoft Headless Design Guidelines.

System Management BIOS Reference Specification.

Glossary

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

Word / Acronym	Definition
ACPI	Advanced Configuration and Power Interface. ACPI is an open industry specification proposed by Intel, Microsoft and Toshiba. ACPI enables and supports reliable power management through improved hardware and operating system coordination. For more information, see ACPI_1.0b or ACPI_2.0.
ANSI	American National Standards Institute.
AP	Application Processor.
API	Application Programming Interface. A software abstraction provided by the BIOS to applications and/or the Operating System.
ASCII	American Standard Code for Information Interchange. An 8-level code (7 bits plus parity check) widely used in data processing and data communications systems.
BEV	BootStrap Entry Vector
BIOS	Basic Input/Output System. The firmware (Software embedded into hardware) that is used to boot the processors and initialize the chipset and I/O of the system prior to handing off control of execution to the OS.
BMC	Baseboard Management Controller.
BSP	Boot Strap Processor. The processor selected at boot time to be the primary processor in a multi-processor system.
COM1	Communication Port 1, serial port 1.
COM2	Communication Port 2, serial port 2.
DIMM	Dual In-line Memory Module.
DPC	Direct Platform Control. Remote Server Management over the network or serial port regardless the status of the server’s operating system or power state.
ECC	Error Correction Code. Refers to a memory system that has extra bit(s) to support limited detection/correction of memory errors.
EFI	Extensible Firmware Interface. A new hardware/OS interface for the BIOS to utilize in the bootup of the system.
EMP	Emergency Management Port.
Firmware	Any software that is permanently stored in an integrated circuit and used by the hardware for basic initialization or operation.
FRB	Fault Resilient Booting. A hardware/firmware method to boot past any fault that would not prevent that system from otherwise operating.
FRU	Field Replaceable Unit.
FWH	Firmware Hub. Physical storage hardware circuitry for the system firmware.
GB	Gigabyte. 1024 Megabytes or 2^30 bytes.
GCM	Generic Communication Module.
GUID	Globally Unique Identifier.
HT Technology	Hyper-Threading Technology
I/O	Input/Output.
I2O	Intelligent I/O. An open architecture for the development of device drivers in network system environments
IHS	Integrated Heat Spreader. The metallic surface covering of a processor package intended to encourage the flow of heat away from the processor die and to the heatsink.

Word / Acronym	Definition
IMI	Independent Memory Interface.
IOP	I2O-compliant I/O Platforms. These typically contain an I/O processor and I/O subsystem.
IPMB	Intelligent Platform Management Buses.
IPMI	Intelligent Platform Management Interface. An industry standard that defines standardized, abstracted interfaces to platform management hardware. See IPMI_1.5 and IPMI_2.0.
KB	Kilobyte. 2^10=1024 bytes.
KCS	Keyboard Controller Style.
LAN	Local Area Network.
LED	Light Emitting Diode.
LPC	Low Pin Count.
MB	Megabyte. 1024 Kilobytes or 2^20 bytes.
NB	Northbridge. The component of the chipset that interfaces the processors to memory and I/O.
NIC	Network Interface Controller/Card.
NMI	Non-Maskable Interrupt.
ODT	On-Die Termination.
OPROM	Option ROM. Used to describe the code provided by hardware vendors to provide support for integrated devices or add-in adapters.
PEF	Platform Event Filtering.
PET	Platform Event Trap.
PLD	Programmable Logic Device.
PME	Power Management Event.
PnP	Plug and Play. See PnP_BIOS and PnP_ISA.
POST	Power-on Self Test.
PXE	Pre-boot eXecution Environment. This is the system envirionment when EFI firmware is executing during boot and in control of system resources.
PXH	PCI Express* to PCI-X* bridge hub.
RAID	Redundent Array of Independent Disks.
RAS	Reliability, Availability, and Serviceability
ROMB	RAID on Motherboard.
SATA	Serial-ATA.
SDR	Sensor Data Record.
SDRAM	Synchronous DRAM. A type of DRAM that uses an external clock and supports faster memory access than prior DRAM memory types.
SEL	System Event Log.
SMI	System Management Interrupt. A special type of interrupt to signal attention from the SMI handler.
SOL	Serial Over LAN.
SPD	Serial Presence Detect.
TIM	Thermal Interface Material. Replaces thermal grease between the IHS and the heatsink.
USB	Universal Serial Bus, a standard serial expansion bus meant for connecting peripherals.
VRD	Voltage Regulator Down. Voltage regulation circuitry built into the main board.
VRM	Voltage Regulation Module. Voltage regulation circuitry that can be added to the main board on a plug-in module.
WOL	Wake On LAN.
XMB	eXternal Memory Bridge (a component of the Intel® E8501 Chipset)