Intel® Server Board SE7520JR2

Technical Product Specification

Revision 1.0

October 2004

Enterprise Platforms and Services Marketing

Revision History

Date	Revision Number	Modifications
December 2003	0.5	Preliminary Release
June 2004	0.9	Memory Sub-system rewrite, BIOS Chapter Updated, Management Chapter re-write, Error Handling chapter re-write, several changes made to better reflect final design
October 2004	1.0	First non-NDA release; Updated IRQ routing diagrams, Updated mBMC Sensor tables, Updates to Regulatory Information, Updated Sensor data tables

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 Intel® Server Board SE7520JR2 may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

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

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

Intel Corporation server boards contain a number of high-density VLSI and power delivery components that need adequate airflow to cool. Intel's own chassis are designed and tested to meet the intended thermal requirements of these components when the fully integrated system is used together. It is the responsibility of the system integrator that chooses not to use Intel developed server building blocks to consult vendor datasheets and operating parameters to determine the amount of 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, Pentium, Itanium, and Xeon are trademarks or registered trademarks of Intel Corporation.

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

Table of Contents

List of Figures

List of Tables

< This page intentionally left blank. >

1. Introduction

This Technical Product Specification (TPS) provides detail to the architecture and feature set of the Intel® Server Board SE7520JR2.

The target audience for this document is anyone wishing to obtain more in depth detail of the server board than what is generally made available in the board's Users Guide. It is a technical document meant to assist people with understanding and learning more about the specific features of the board.

This is one of several technical documents available for this server board. All of the functional sub-systems that make up the board are described in this document. However, some low-level detail of specific sub-systems is not included. Design level information for specific sub-systems can be obtained by ordering the External Product Specification (EPS) for a given sub-system. The EPS documents available for this server board include the following:

- Intel® Server Board SE7520JR2 BIOS EPS
- Intel® Server Board SE7520JR2 Baseboard Management Controller EPS
- mini Baseboard Management Controller (mBMC) Core EPS for IPMI-based Systems
- Sahalee Core BMC EPS for IPMI v1.5

These documents are not publicly available and must be ordered by your local Intel representative.

1.1 Chapter Outline

This document is divided into the following chapters

- Chapter 1 – Introduction
- Chapter 2 – Product Overview
- Chapter 3 – Board Architecture
- Chapter 4 – System BIOS
- Chapter 5 – Platform Management Architecture
- Chapter 6 – Error Reporting and Handling
- Chapter 7 – Connector Pin-out and Jumper Blocks
- Chapter 8 – Environmental Specifications
- Chapter 9 – Miscellaneous Board Information
- Appendix A – Integration and Usage Tips

1.2 Server Board Use Disclaimer

Intel Corporation server boards contain a number of high-density VLSI and power delivery components that need adequate airflow to cool. Intel ensures through its own chassis development and testing that when Intel server building blocks are used together, the fully integrated system will meet the intended thermal requirements of these components. It is the responsibility of the system integrator who chooses not to use Intel developed server building blocks to consult vendor datasheets and operating parameters to determine the amount of 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.

2. Server Board Overview

The Intel® Server Board SE7520JR2 is a monolithic printed circuit board with features that were designed to support the high density 1U and 2U server markets.

2.1 Server Board SE7520JR2 SKU Availability

In this document, the name SE7520JR2 is used to describe the family of boards that are made available under a common product name. The core features for each board will be common; however each board will have the following distinctions:

Product Code	Feature Distinctions
SE7520JR2SCSID2	Onboard SCSI + Onboard SATA (RAID) + DDR2 – 400 MHz
SE7520JR2SCSID1	Onboard SCSI + Onboard SATA (RAID) + DDR – 266/333 MHz
SE7520JR2ATAD2	Onboard SATA (RAID) + DDR2 – 400 MHz
SE7520JR2ATAD1	Onboard SATA (RAID) + DDR – 266/333 MHz

Throughout this document, all references to the Server Board SE7520JR2 will refer to all four board SKUs unless specifically noted otherwise. The board you select to use, may or may not have all the features described based on the listed board differences.

2.2 Server Board SE7520JR2 Feature Set

- Dual processor slots supporting 800MHz Front Side Bus (FSB) Intel® Xeon™ processors
- Intel E7520 Chipset (MCH, PXH, ICH5-R)
- Two PCI riser slots
    - Riser Slot 1: Supports low profile PCI-X 66/100MHz PCI-X cards
    - Riser Slot 2: Using Intel® adaptive slot technology and different riser cards, this slot is capable of supporting full height PCI-X 66/100/133 or PCI-Express cards.
- Six DIMM slots supporting DDR2 – 400MHz DIMMs or DDR – 266/333 MHz[1] DIMMs
- Dual channel LSI* 53C1030 Ultra320 SCSI Controller with integrated RAID 0/1 support (SCSI SKU only)
- Dual Intel® 82546GB 10/100/1000 Network Interface Controllers (NICs)
- On board ATI* Rage XL video controller with 8MB SDRAM
- On-board platform instrumentation using a National* PC87431M mini-BMC
- External IO connectors
    - Stacked PS2 ports for keyboard and mouse

[1] The use of DDR2 - 400 MHz or DDR - 266/333 MHz DIMMs is dependant on which board SKU is used. DDR-2 DIMMs cannot be used on a board designed to support DDR. DDR DIMMs cannot be used on boards designed to support DDR-2.

  - RJ45 Serial B Port
  - Two RJ45 NIC connectors
  - 15-pin video connector
  - Two USB 2.0 ports
  - U320 High density SCSI connector (Channel B) (SCSI SKU only)
- Internal IO Connectors / Headers
  - Two onboard USB port headers. Each header is capable of supporting two USB 2.0 ports.
  - One 10-pin DH10 Serial A Header
  - One Ultra320 68-pin SCSI Connector (Channel A) (SCSI SKU only)
  - Two SATA connectors with integrated chipset RAID 0/1 support
  - One ATA100 connector
  - One floppy connector
  - SSI-compliant (34-pin) and custom control panel headers (50-pin and 100-pin)
  - SSI-compliant 24-pin main power connector. This supports ATX-12V standard in the first 20 pins
  - Intel® Management Module (IMM) connector supporting both Professonal Edition and Advanced Edition management modules
- Intel® Light-Guided Diagnostics on all FRU devices (processors, memory, power)
- Port-80 Diagnostic LEDs displaying POST codes

The following figure shows the board layout of the Server Board SE7520JR2. Each connector and major component is identified by number and is identified in Table 1.

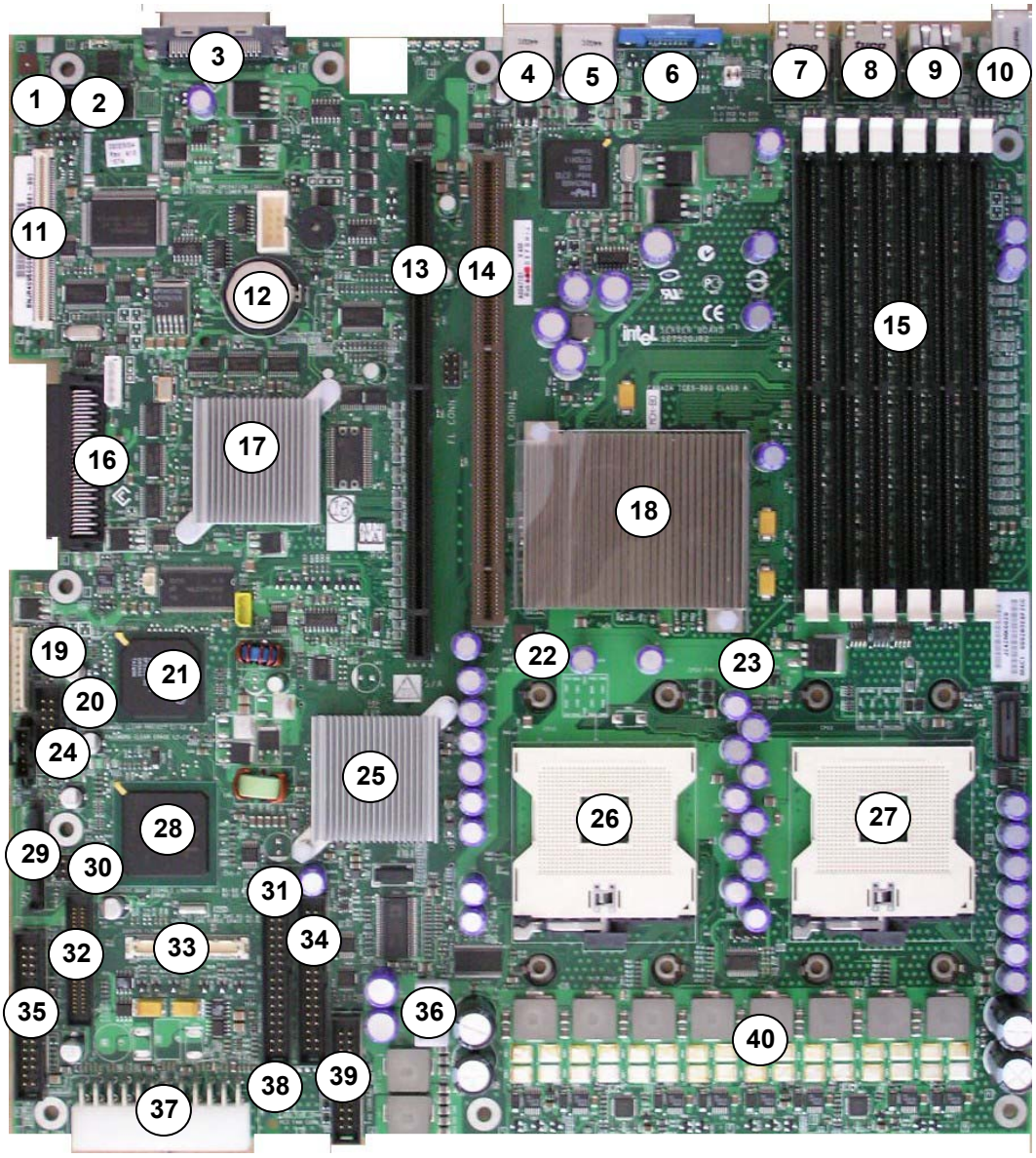


Figure 1. SE7520JR2 Board Layout

Table 1: Baseboard Layout Reference

Ref #	Description	Ref #	Description
1	(J1A1) 2-Pin Chassis Intrusion Header (J1A2) 2-Pin Hard Drive Act LED Header (J1A4) Rolling BIOS Jumper	22	CPU #2 Fan Header
2	10-Pin DH10 Serial A Header	23	CPU #1 Fan Header
3	Ext SCSI Channel B Connector	24	5-pin Power Sense Header
4	USB Port 2	25	PXH – Chipset Component
5	USB Port 1	26	CPU #2 Socket
6	Video Connector	27	CPU #1 Socket
7	NIC #2	28	ICH5-R – Chipset Component
8	NIC #1	29	SATA Ports
9	RJ-45 Serial B Port	30	(J1H2) Recovery Boot Jumper (J1H3) Password Clear Jumper (J1H4) CMOS Clear Jumper
10	Stacked PS/2 Keyboard and Mouse Ports	31	Legacy ATA-100 connector
11	Intel Management Module Connector	32	50-pin Control Panel Header
12	CMOS Battery	33	100-pin Control Panel, Floppy, IDE Connector
13	Full Height Riser Card Slot	34	Legacy Floppy Connector
14	Low Profile Riser Card Slot	35	SSI 34-pin Control Panel Header
15	DIMM Slots	36	8-Pin AUX Power Connector
16	68-pin SCSI Channel A Connector	37	24-Pin Main Power Connector
17	LSI 53C1030 SCSI Controller	38	SSI System Fan Header
18	MCH – Chipset Component	39	SR1400/SR2400 System Fan Header
19	1x10 USB Header	40	Processor Voltage Regulator Circuitry
20	2x5 USB Header		
21	ATI RageXL Video Controller		

The following mechanical drawing shows the physical dimensions of the baseboard.

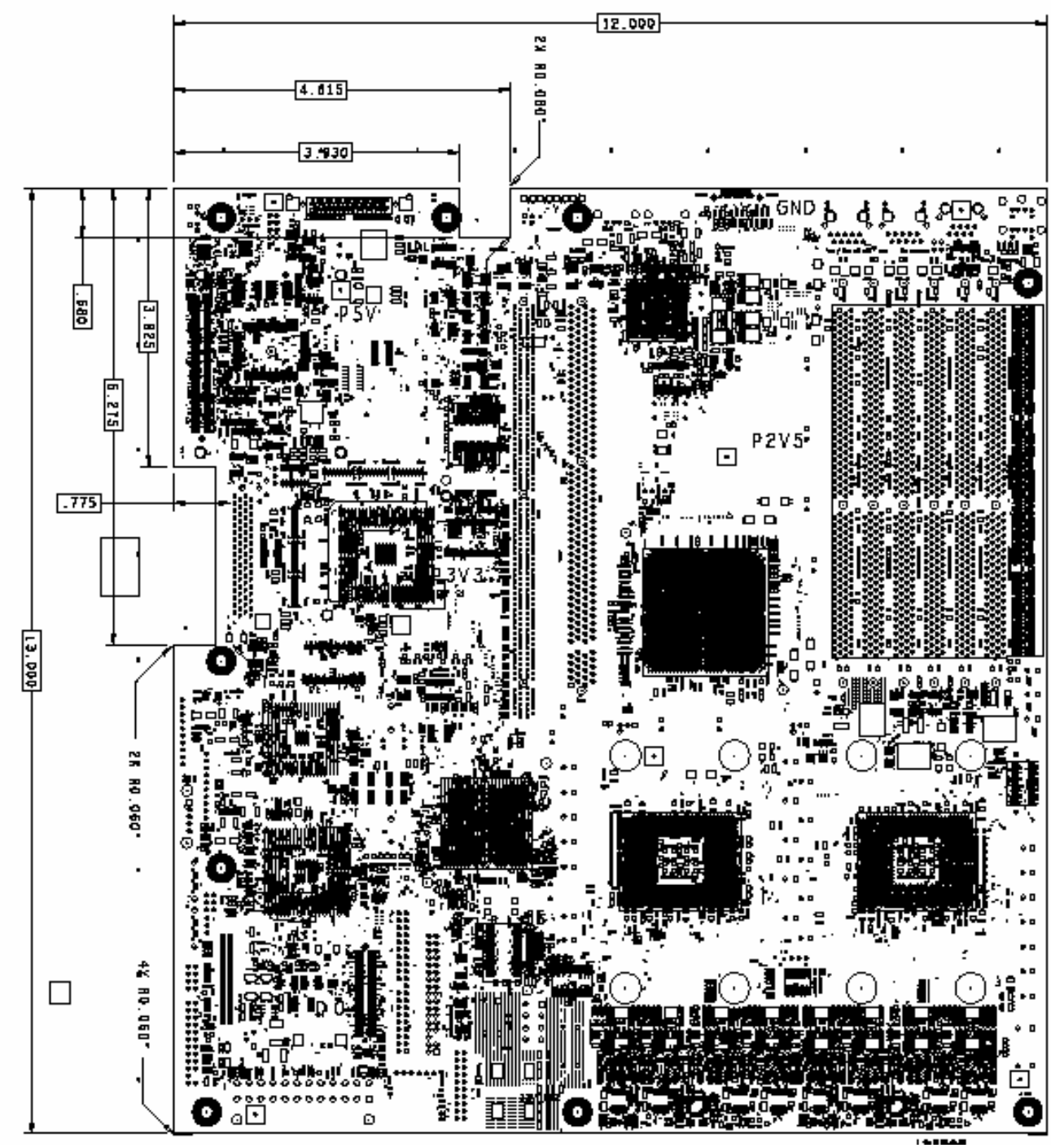


Figure 2. Server Board Dimensions

3. Functional Architecture

This chapter provides a high-level description of the functionality associated with the architectural blocks that make up the Intel Server Board SE7520JR2.

Note: This document describes the features and functionality of the Server Board SE7520JR2 when using standard on-board platform instrumentation. Some functionality and feature descriptions change when using either the Professional Edition or Advanced Edition Intel Management Modules. Functional changes when either of these two options are used are described in a separate document.

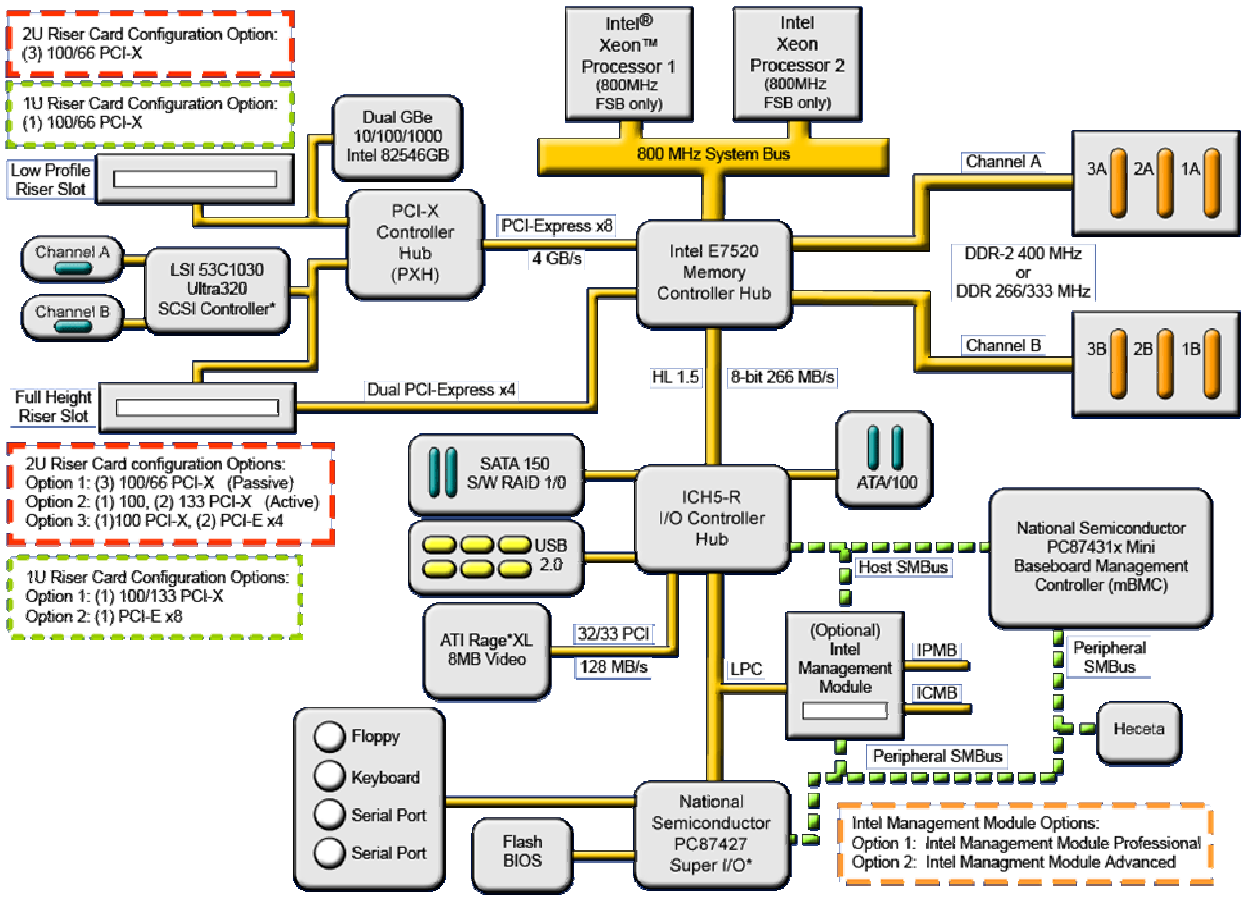


Figure 3. Server Board SE7520JR2 Block Diagram

3.1 Processor Sub-system

The support circuitry for the processor sub-system consists of the following:

- Dual 604-pin zero insertion force (ZIF) processor sockets
- Processor host bus AGTL+ support circuitry
- Reset configuration logic
- Processor module presence detection logic
- BSEL detection capabilities
- CPU signal level translation
- Common Enabling Kit (CEK) CPU retention support

3.1.1 Processor Voltage Regulators

The baseboard has two VRDs (Voltage Regulator Devices) providing the appropriate voltages to the installed processors. Each VRD is compliant with the VRD 10.1 specification and is designed to support Intel® Xeon™ processors that require up to a sustained maximum of 105 AMPs and peak support of 120A.

The baseboard supports the current requirements and processor speed requirements defined in the Flexible Mother Board (FMB) specification for all 800 MHz FSB Intel Xeon processors. FMB is an estimation of the maximum values the 800 MHz FSB versions of the Intel Xeon processors will have over their lifetime. The value is only an estimate and actual specifications for future processors may differ. At present, the current demand per FMB is a sustained maximum of a 105 Amps and peak support of 120 Amps.

3.1.2 Reset Configuration Logic

The BIOS determines the processor stepping, cache size, etc through the CPUID instruction. All processors in the system must operate at the same frequency; have the same cache sizes; and same VID. No mixing of product families is supported. Processors run at a fixed speed and cannot be programmed to operate at a lower or higher speed.

3.1.3 Processor Module Presence Detection

Logic is provided on the baseboard to detect the presence and identity of installed processors. In dual-processor configurations, the on-board mini Baseboard Management Controller (mBMC) must read the processor voltage identification (VID) bits for each processor before turning on the VRD. If the VIDs of the two processors are not identical, then the mBMC will not turn on the VRD. Prior to enabling the embedded VRD, circuitry on the baseboard ensures that the following criteria are met:

- In a uni-processor configuration, CPU 1 is installed
- Only supported processors are installed in the system to prevent damage to the MCH
- In dual processor configurations, both processors support the same FSB frequency

3.1.4 GTL2006

The GTL2006 is a 13-bit translator designed for 3.3V to GTL/GTL+ translations to the system bus. The translator incorporates all the level shifting and logic functions required to interface between the processor subsystem and the rest of the system.

3.1.5 Common Enabling Kit (CEK) Design Support

The baseboard has been designed to comply with Intel's Common Enabling Kit (CEK) processor mounting and heat sink retention solution. The baseboard will ship with a CEK spring snapped onto the bottom side of the board beneath each processor socket. The CEK spring is removable, allowing for the use of non-Intel heat sink retention solutions.

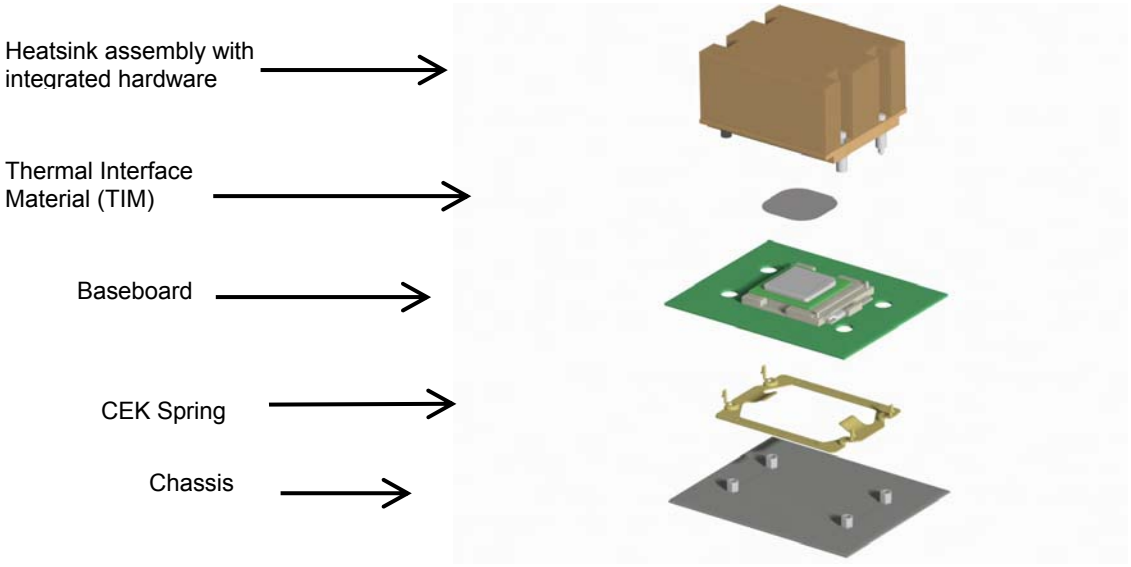


Figure 4. CEK Processor Mounting

3.1.6 Processor Support

The Server Board SE7520JR2 is designed to support one or two Intel® Xeon™ processors utilizing an 800 MHz front side bus with frequencies starting at 2.8 GHz. Previous generations of Intel Xeon processor are not supported on the Server Board SE7520JR2.

The server board is designed to provide up to 120A peak per processors. Processors with higher current requirements are not supported.

Note: Only Intel® Xeon™ processors that support an 800MHz Front Side Bus are supported on the Server Board SE7520JR2. See the following table for a list of supported processors and their operating frequencies.

Table 2: Processor Support Matrix

Processor Family	FSB Frequency	Frequency	Support
Intel® Xeon™	533 MHz	2.8 GHz	No
Intel® Xeon™	533 MHz	3.06 GHz	No
Intel® Xeon™	533 MHz	3.2 GHz	No
Intel® Xeon™	800 MHz	2.8 GHz	Yes
Intel® Xeon™	800 MHz	3.0 GHz	Yes

Processor Family	FSB Frequency	Frequency	Support
Intel® Xeon™	800 MHz	3.2 GHz	Yes
Intel® Xeon™	800 MHz	3.4 GHz	Yes
Intel® Xeon™	800 MHz	3.6 GHz	Yes

3.1.6.1 Processor Mis-population Detection

The processors must be populated in the correct order for the processor front-side bus to be correctly terminated. CPU socket 1 must be populated before CPU socket 2. Baseboard logic will prevent the system from powering up if a single processor is present but it is not in the correct socket. This protects the logic against voltage swings or unreliable operation that could occur on an incorrectly terminated front-side bus.

If processor mis-population is detected when using standard on-board platform instrumentation, the mBMC will log an error against processor 1 to the System Event Log; Configuration Error, and the baseboard hardware will illuminate both processor error LEDs. If an IMM (Professional or Advanced editions) is used in systems, the Sahalee BMC will generate a series of beep codes when this condition is detected and the BMC will illuminate the processor 1 fault LED.

3.1.6.2 Mixed Processor Steppings

For optimum system performance, only identical processors should be installed in a system. Processor steppings within a common processor family can be mixed in a system provided that there is no more than a 1 stepping difference between them. If the installed processors are more than 1 stepping apart, an error is reported. Acceptable mixed steppings are not reported as errors by the BIOS.

3.1.6.3 Mixed Processor Models

Processor models cannot be mixed in a system. If this condition is detected an error (8196) is logged in the SEL. An example of a faulty processor configuration may be when one installed processor supports a 533MHz front side bus while the other supports an 800MHz front side bus.

3.1.6.4 Mixed Processor Families

Processor families cannot be mixed in a system. If this condition is detected an error (8194) is logged in the SEL.

3.1.6.5 Mixed Processor Cache Sizes

If the installed processors have mixed cache sizes, an error (8192) will be logged in the SEL and an error (196) is reported to the Management Module. The size of all cache levels must match between all installed processors. Mixed cache processors are not supported.

3.1.6.6 Jumperless Processor Speed Settings

The Intel® Xeon™ processor does 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 Ratio register is programmed with the value read from the High Ratio register. If all processors do not match, the highest common value between

High and Low Ratio is determined and programmed to 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.

3.1.6.7 Microcode

IA-32 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 non-volatile 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 supports variable size microcode updates. The BIOS verifies the signature prior to storing the update in the flash.

3.1.6.8 Processor Cache

The BIOS enables all levels of processor cache as early as possible during POST. There are no user options to modify the cache configuration, size or policies. The largest and highest level cache detected is reported in BIOS Setup.

3.1.6.9 Hyper-Threading Technology

Intel® Xeon™ processors support Hyper-Threading Technology. The BIOS detects processors that support this feature and enables the feature during POST. BIOS Setup provides an option to selectively enable or disable this feature. The default behavior is “Enabled”.

The BIOS creates additional entries in the ACPI MP tables to describe the virtual processors. The SMBIOS Type 4 structure shows only the physical processors installed. It does not describe the virtual processors because some operating systems are not able to efficiently utilize the Hyper-Threading Technology.

3.1.6.10 Intel® SpeedStep® Technology

Intel® Xeon™ processors support the Geyserville3 (GV3) (whether Geyserville3 is an Intel internal code name?) feature of the 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 BIOS implements the GV3 feature in conjunction with the TM2 feature.

3.1.6.11 EM64T Technology Support

The system BIOS on the Server Board SE7520JR2 supports the Intel Extended Memory 64 technology (EM64T) of the Intel® Xeon™ Processors. There is no BIOS setup option to enable or disable this support. The system will be in IA-32 compatibility mode when booting to an OS. To utilize this feature, a 64-bit capable OS and OS specific drivers are needed.

3.1.7 Multiple Processor Initialization

IA-32 processors have a microcode-based bootstrap processor (BSP) arbitration protocol. On reset, all of the processors compete to become the BSP. If a serious error is detected during its Built-in Self-Test (BIST), that processor does not participate in the initialization protocol. A single processor that successfully passes BIST is automatically selected by the hardware as the

BSP and starts executing from the reset vector (F000:FFF0h). A processor that does not perform the role of BSP is referred to as an application processor (AP).

The BSP is responsible for executing the BIOS power-on self-test (POST) and preparing the machine to boot the 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 (PIC) and non-maskable interrupt (NMI)).

As a part of the boot process, the BSP enables the application processor. When enabled, the AP programs its Memory Type Range Registers (MTRRs) to be identical to those of the BSP. The AP executes a halt instruction with its local interrupts disabled. If the BSP determines that an AP exists that is a lower-featured processor or that has a lower value returned by the CPUID function, the BSP switches to the lowest-featured processor in the system.

3.1.8 CPU Thermal Sensors

The CPU temperature will be indirectly measured via thermal diodes. These are monitored by the LM93 sensor monitoring device. The mBMC configures the LM93 to monitor these sensors. The temperatures are available via mBMC IPMI sensors.

3.1.9 Processor Thermal Control Sensor

The Intel Xeon processors generate a signal to indicate throttling due to a processor over temp condition. The mBMC implements an IPMI sensor that provides the percentage of time a processor has been throttled over the last 1.46 seconds. Baseboard management forces a thermal control condition when reliable system operation requires reduced power consumption.

3.1.10 Processor Thermal Trip Shutdown

If a thermal overload condition exists (thermal trip), the processor outputs a digital signal that is monitored by the baseboard management sub-system. A thermal trip is a critical condition and indicates that the processor may become damaged if it continues to run. To help protect the processor, the management controller automatically powers off the system. In addition the System Status LED will change to Amber and the error condition will be logged to the System Event Log (SEL).

If either the Intel Management Module Professional Edition or Advanced Edition is present in the system, the Fault LED fro the affected processor will also be illuminated.

3.1.11 Processor IERR

The IERR signal is asserted by the processor as the result of an internal error. The mBMC configures the LM93 device to monitor this signal. When this signal is asserted, the mBMC generates a processor IERR event.

3.2 Intel® E7520 Chipset

The architecture of the Server Board SE7520JR2 is designed around the Intel E7520 chipset. The chipset consists of three components that together are responsible for providing the interface between all major sub-systems found on the baseboard, including the processor, memory, and I/O sub-systems. These components are:

  - Memory Controller Hub (MCH)
  - I/O Controller Hub (ICH5-R)
- PCI-X Hub (PXH)

The following sub-sections provide an overview of the primary functions and supported features of each chipset component as they are used on the Server Board SE7520JR2. Later sections in this chapter provide more detail on the implementation of the sub-systems.

3.2.1 Memory Controller Hub (MCH)

The MCH integrates four functions into a single 1077-ball FC-BGA package:

- Front Side Bus
- Memory Controller
- PCI-Express Controller
- Hub Link Interface

3.2.1.1 Front Side Bus (FSB)

The E7520 MCH supports either single or dual processor configurations using 800MHz FSB Intel Xeon processors. The MCH supports a base system bus frequency of 200 MHz. The address and request interface is double pumped to 400 MHz while the 64-bit data interface (+ parity) is quad pumped to 800 MHz. This provides a matched system bus address and data bandwidths of 6.4 GB/s

3.2.1.2 MCH Memory Sub-System Overview

The MCH provides an integrated memory controller for direct connection to two channels of registered DDR-266, DDR-333 or DDR2-400 memory (stacked or unstacked). Peak theoretical memory data bandwidth using DDR266 technology is 4.26 GB/s and 5.33 GB/S for DDR333 technology. For DDR2-400 technology, this increases to 6.4 GB/s.

Several RASUM (Reliability, Availability, Serviceability, Usability, and Manageability) features are provided by the E7520 MCH memory interface.

- Memory mirroring allows two copies of all data in the memory subsystem to be maintained (one on each channel).
- DIMM sparing allows one DIMM per channel to be held in reserve and brought on-line if another DIMM in the channel becomes defective. DIMM sparing and memory mirroring are mutually exclusive.
- Hardware periodic memory scrubbing, including demand scrub support.
- Retry on uncorrectable memory errors.
- x4 SDDC for memory error detection and correction of any number of bit failures in a single x4 memory device.

3.2.1.3 PCI Express

The E7520 MCH is the first Intel chipset to support the new PCI Express* high-speed serial I/O interface for superior I/O bandwidth. The scalable PCI Express interface complies with the PCI Express Interface Specification, Rev 1.0a. On the Server Board SE7520JR2, two of the three available x8 PCI Express interfaces are used, each with a maximum theoretical bandwidth of 4

GB/s. One x8 interface is used as the interconnect between the MCH and PXH, while the other is configured as two separate x4 interfaces to the full height riser slot.

The E7520 MCH is a root class component as defined in the PCI Express Interface Specification, Rev 1.0a. The PCI Express interfaces of the MCH support connection to a variety of bridges and devices compliant with the same revision of the specification. Refer to the *Server Board SE7520JR2 Tested Hardware and OS List* for the add-in cards tested on this platform.

3.2.1.4 Hub Interface

The MCH interfaces with the Intel 82801ER I/O Controller Hub 5-R (ICH5-R) via a dedicated Hub Interface which supports a peak bandwidth of 266MB/s using a x4 base clock of 66 MHz.

3.2.2 PCI-X Hub (PXH)

The PXH provides the data interface between the MCH and two PCI-X bus segments over a high-speed PCI-Express x8 link. The PCI-Express interface is compliant with the PCI Express Base Specification rev 1.0 and provides a maximum realized bandwidth of 2GB/s in each direction simultaneously, for an aggregate of 4 GB/s.

The PCI-X interfaces of the PXH comply with the following:

- PCI-X Addendum to the PCI Local Bus Specification Revision 1.0b
- Mode 1 of the PCI-X Electrical and Mechanical Addendum to the PCI Local Bus Specification Revision 2.0a
- PCI-X Protocol Addendum to the PCI Local Bus Specification Revision 2.0a

For conventional PCI Mode, the PXH supports PCI bus frequencies of 66 MHz, 100 MHz, and 133 MHz.

On the Server Board SE7520JR2 each of the two PCI-X interfaces (PCI Bus A and PCI Bus B) is independently controlled to operate in either a conventional PCI or PCI-X mode. PCI Bus A is routed to control I/O from the full-height riser slot and the LSI* 53C1030 Dual Channel SCSI controller and is capable of supporting both PCI-X Mode 1 and Mode 2 interfaces depending on the riser card used. PCI Bus B is routed to control I/O from the low profile riser slot and the 82546GB Dual GB Ethernet controllers.

3.2.2.1 Full-height Riser Slot

Using Intel® Adaptive Slot Technology, the full height riser slot is a proprietary 280-pin slot connector with both PCI-X signals from the PXH and PCI-Express signals from the MCH routed to it. Depending on the riser card used, the slot is able to support both PCI-X and/or PCI-Express add-in cards. The board placement of this slot allows risers to support full-height, full-length add-in cards.

3.2.2.2 Low Profile Riser Slot

The low profile riser slot is a standard 202-pin slot connector supporting PCI-X signals from the PXH. Because of available board clearances, riser cards can only support low-profile add-in cards with this slot.

3.2.2.3 I/OxAPIC Controller

The PXH contains two I/OxAPIC controllers, both of which reside on the primary bus. The intended use of these controllers is to have the interrupts from PCI bus A connected to the interrupt controller on device 0, function 1 and have the interrupts on PCI bus B connected to the interrupt controller on device 0, function 3.

3.2.2.4 SMBus Interface

The SMBus interface can be used for system and power management related tasks. The interface is compliant with System Management Bus Specification Revision 2.0. The SMBus interface allows full read/write access to all configuration and memory spaces in the PXH.

3.2.3 I/O Controller Hub (ICH5-R)

The ICH5-R is a multi-function device providing an upstream hub interface for access to several embedded I/O functions and features including:

- PCI Local Bus Specification, Revision 2.3 with support for 33 MHz PCI operations.
- ACPI power management logic support
- Enhanced DMA controller, interrupt controller, and timer functions
- Integrated IDE controller with support for Ultra ATA100/66/33
- Integrated SATA controller
- USB host interface with support for eight USB ports; four UHCI host controllers; one EHCI high-speed USB 2.0 host controller
- System Management Bus (SMBus) Specification, Version 2.0 with additional support for I^2C devices
- Low Pin Count (LPC) interface
- Firmware Hub (FWH) interface support

Each function within the ICH5-R has its own set of configuration registers. Once configured, each appears to the system as a distinct hardware controller sharing the same PCI bus interface.

3.2.3.1 PCI Interface

The ICH5-R PCI interface provides a 33 MHz, Revision 2.3 compliant implementation. All PCI signals are 5-V tolerant, except PME#. The ICH5 integrates a PCI arbiter that supports up to six external PCI bus masters in addition to the internal ICH5 requests. On the Server Board SE7520JR2 this PCI interface is used to support on-board PCI devices including the ATI* video controller, Super I/O chip, and hardware monitoring sub-system.

3.2.3.2 IDE Interface (Bus Master Capability and Synchronous DMA Mode)

The fast IDE interface supports up to four IDE devices, providing an interface for IDE hard disks and ATAPI devices. Each IDE device can have independent timings. The IDE interface supports PIO IDE transfers up to 16 Mbytes/sec and Ultra ATA transfers up 100 Mbytes/sec. It does not consume ISA DMA resources. The IDE interface integrates 16x32-bit buffers for optimal transfers. The ICH5-R's IDE system contains two independent IDE signal channels. They can be electrically isolated independently. They can be configured to the standard primary and secondary channels (four devices). The Server Board SE7520JR2 provides interfaces to both

IDE channels of the ICH5R. One channel is accessed through the 40-pin connector on the baseboard. The signals of the second channel are routed to the 100-pin backplane connector for use in either the Intel Server Chassis SR1400 or SR2400 when integrated with a backplane for slim-line optical drive use.

3.2.3.3 SATA Controller

The SATA controller supports two SATA devices, providing an interface for SATA hard disks and ATAPI devices. The SATA interface supports PIO IDE transfers up to 16 Mb/s and Serial ATA transfers up to 1.5 Gb/s (150 MB/s). The ICH5-R's SATA system contains two independent SATA signal ports. They can be electrically isolated independently. Each SATA device can have independent timings. They can be configured to the standard primary and secondary channels.

3.2.3.4 Low Pin Count (LPC) Interface

The ICH5-R implements an LPC Interface as described in the Low Pin Count Interface Specification, Revision 1.1. The Low Pin Count (LPC) bridge function of the ICH5-R resides in PCI Device 31:Function 0. In addition to the LPC bridge interface function, D31:F0 contains other functional units including DMA, interrupt controllers, timers, power management, system management, GPIO, and RTC.

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

The DMA controller incorporates the logic of two 82C37 DMA controllers, with seven independently programmable channels. Channels 0–3 are hardwired to 8-bit, count-by-byte transfers, and channels 5–7 are hardwired to 16-bit, count-by-word transfers. Any two of the seven DMA channels can be programmed to support fast Type-F transfers.

The ICH5-R supports two types of DMA: LPC and PC/PCI. LPC DMA and PC/PCI DMA use the ICH5-R's DMA controller. The PC/PCI protocol allows PCI-based peripherals to initiate DMA cycles by encoding requests and grants via two PC/PC REQ#/GNT# pairs. LPC DMA is handled through the use of the LDRQ# lines from peripherals and special encoding on LAD[3:0] from the host. Single, Demand, Verify, and Increment modes are supported on the LPC interface. Channels 0–3 are 8 bit channels. Channels 5–7 are 16 bit channels. Channel 4 is reserved as a generic bus master request.

The timer/counter block contains three counters that are equivalent in function to those found in one 82C54 programmable interval timer. These three counters are combined to provide the system timer function, and speaker tone. The 14.31818 MHz oscillator input provides the clock source for these three counters.

The ICH5-R provides an ISA-compatible Programmable Interrupt Controller (PIC) that incorporates the functionality of two 82C59 interrupt controllers. The two interrupt controllers are cascaded so 14 external and two internal interrupts are possible. In addition, the ICH5-R supports a serial interrupt scheme. All of the registers in these modules can be read and restored. This is required to save and restore the system state after power has been removed and restored to the platform.

3.2.3.6 Advanced Programmable Interrupt Controller (APIC)

In addition to the standard ISA-compatible PIC described in the previous section, the ICH5-R incorporates the Advanced Programmable Interrupt Controller (APIC).

3.2.3.7 Universal Serial Bus (USB) Controller

The ICH5-R contains an Enhanced Host Controller Interface (EHCI) for Universal Serial Bus, Revision 1.0-compliant host controller that supports USB high-speed signaling. The high-speed USB 2.0 allows data transfers up to 480 Mb/s, which is 40 times faster than full-speed USB.

The ICH5-R also contains four Universal Host Controller Interface (UHCI) controllers that support USB full-speed and low-speed signaling. On the Server Board SE7520JR2, the ICH5-R provides six USB 2.0 ports. All six ports are high-speed, full-speed, and low-speed capable. ICH5-R's port-routing logic determines whether a USB port is controlled by one of the UHCI controllers or by the EHCI controller.

3.2.3.8 RTC

The ICH5-R contains a Motorola* MC146818A-compatible real-time clock with 256 bytes of battery backed RAM. The real-time clock performs two key functions: keeping track of the time of day and storing system data, even when the system is powered down. The RTC operates on a 32.768 KHz crystal and a separate 3 V lithium battery.

The RTC supports two lockable memory ranges. By setting bits in the configuration space, two 8-byte ranges can be locked to read and write accesses. This prevents unauthorized reading of passwords or other system security information.

The RTC supports a date alarm that allows for scheduling a wake up event up to 30 days in advance.

3.2.3.9 General Purpose I/O (GPIO)

Various general-purpose inputs and outputs are provided for custom system design. The number of inputs and outputs varies depending on the ICH5-R configuration. All unused GPI pins are either pulled high or low, so that they are at a predefined level and do not cause undue side effects.

3.2.3.10 Enhanced Power Management

The ICH5-R's power management functions include enhanced clock control, local and global monitoring support for 14 individual devices, and various low-power (suspend) states, such as Suspend-to-DRAM and Suspend-to-Disk. A hardware-based thermal management circuit permits software-independent entrance to low-power states. The ICH5-R contains full support for the Advanced Configuration and Power Interface (ACPI) Specification, Revision 2.0b.

3.2.3.11 System Management Bus (SMBus 2.0)

The ICH5-R contains an SMBus host interface that allows the processor to communicate with SMBus slaves. This interface is compatible with most I^2C devices. Special I^2C commands are implemented. The ICH5-R's SMBus host controller provides a mechanism for the processor to initiate communications with SMBus peripherals (slaves).

The ICH5-R supports slave functionality, including the Host Notify protocol. Hence, the host controller supports eight command protocols of the SMBus interface: Quick Command, Send Byte, Receive Byte, Write Byte/Word, Read Byte/Word, Process Call, Block Read/Write, and Host Notify. See the System Management Bus (SMBus) Specification, Version 2.0 for more information.

3.3 Memory Sub-System

The MCH provides an integrated memory controller for direct connection to two channels of registered DDR-266, DDR-333 or DDR2-400 memory (stacked or unstacked). Peak theoretical memory data bandwidth using DDR266 technology is 4.26 GB/s and 5.33 GB/S for DDR333 technology. For DDR2-400 technology, this increases to 6.4 GB/s

The MCH supports a burst length of four, whether in single or dual channel mode. In dual channel mode this results in eight 64-bit chunks (64-byte cache line) from a single read or write. In single channel mode, two reads or writes are required to access a cache line of data.

3.3.1 Memory Sizing

The memory controller is capable of supporting up to 4 loads per channel for DDR-333 and DDR2-400. Memory technologies are classified as being either single rank or dual rank depending on the number of DRAM devices that are used on any one DIMM. A single rank DIMM is a single load device, ie) Single Rank = 1 Load. Dual rank DIMMs are dual load devices, ie) Dual Rank = 2 loads.

The Server Board SE7520JR2 provides the following maximum memory capacities based on the number of DIMM slots provided and maximum supported memory loads by the chipset:

- 24GB maximum capacity for DDR-266
- 16GB maximum capacity for DDR-333 and DDR2-400

The minimum memory supported with the system running in single channel memory mode is:

- 256MB for DDR-266, DDR-333 and DDR2-400

Supported DIMM capacities are as follows:

- DDR-266 Memory DIMM sizes include: 256MB, 512MB, 1GB, 2GB, and 4GB.
- DDR-333 Memory DIMM sizes include: 256MB, 512MB, 1GB, 2GB, and 4GB.
- DDR2-400 Memory DIMM sizes include: 256MB, 512MB, 1GB, 2GB, and 4GB.

DIMM Module Capacities:

SDRAM Parts / SDRAM Technology Used	128Mb	256Mb	512Mb	1Gb
X8, single row	128MB	256MB	512MB	1GB

X8, double row	256MB	512MB	1GB	2GB
X4, single row	256MB	512MB	1GB	2GB
X4, Stacked, double row	512MB	1GB	2GB	4GB

DIMMs on channel ‘A’ are paired with DIMMs on channel ‘B’ to configure 2-way interleaving. Each DIMM pair is referred to as a bank. The bank can be further divided into two rows, based on single-sided or double-sided DIMMs. If both DIMMs in a bank are single-sided, only one row is said to be present. For double-sided DIMMs, both rows are said to be present.

The Server Board SE7520JR2 has six DIMM slots, or three DIMM banks. Both DIMMs in a bank should be identical (same manufacturer, CAS latency, number of rows, columns and devices, timing parameters etc.). Although DIMMs within a bank must be identical, the BIOS supports various DIMM sizes and configurations allowing the banks of memory to be different. Memory sizing and configuration is guaranteed only for qualified DIMMs approved by Intel.

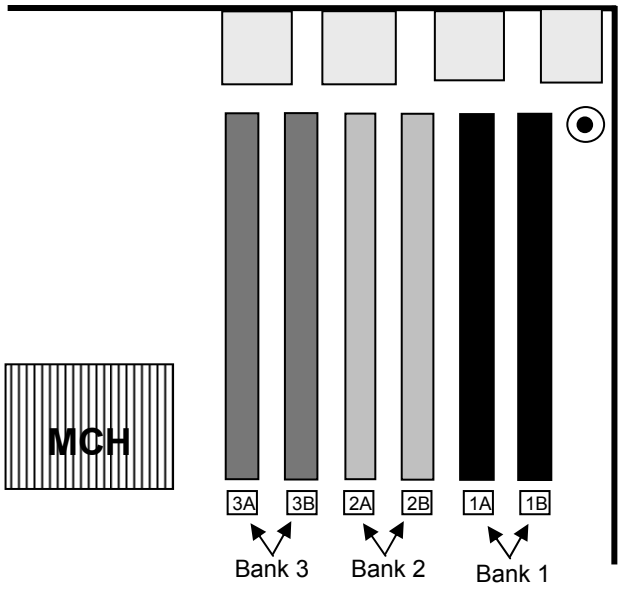


Figure 5. Identifying Banks of Memory

The BIOS reads the Serial Presence Detect (SPD) SEEPROMs on each installed memory module to determine the size and timing of the installed memory modules. The memory-sizing algorithm determines the size of each bank of DIMMs. The BIOS programs the Memory Controller in the chipset accordingly. The total amount of configured memory can be found using BIOS Setup.

3.3.2 Memory Population

Mixing of DDR-266 and DDR-333 DIMMs is supported between banks of memory. However, when mixing DIMM types, DDR-333 will run at DDR-266 speeds.

Using the following algorithm, BIOS configures the memory controller of the MCH to run in either dual channel mode or single channel mode:

(1) If 1 or more fully populated DIMM banks are detected, the memory controller is set to dual channel mode. Otherwise, go to step (2)

(2) If DIMM 1A is present, set memory controller to single channel mode A. Otherwise, go to step (3)

(3) If Channel 1B DIMM is present, set memory controller to single channel mode B. Otherwise, generate a memory configuration error

DDR-266 & DDR-333 DIMM population rules are as follows:

(1) DIMM banks must be populated in order starting with the slots furthest from MCH
(2) Single rank DIMMs must be populated before dual rank DIMMs
(3) A maximum of four DIMMs can be populated when all four DIMMs are dual rank DDR-333 DIMMs.

DDR2 400 DIMM population rules are as follows:

(1) DIMMs banks must be populated in order starting with the slots furthest from MCH
(2) Dual rank DIMMs are populated before single rank DIMMs
(3) A maximum of four DIMMs can be populated when all four DIMMs are dual rank DDR2-400 DIMMs

The following tables show the supported memory configurations.

- s/r = single rank
- d/r = dual rank
- E = Empty

Table 3: Supported DDR-266 DIMM Populations

	Bank 3 – DIMMs 3A, 3B	Bank 2 – DIMMs 2A, 2B	Bank 1 – DIMMs 1A, 1B
MCH	S/R	S/R	S/R
	E	S/R	S/R
	E	E	S/R
	D/R	D/R	D/R
	E	D/R	D/R
	E	E	D/R
	D/R	S/R	S/R
	D/R	D/R	S/R
	E	D/R	S/R

Table 4: Supported DDR-333 DIMM Populations

	Bank 3 – DIMMs 3A, 3B	Bank 2 – DIMMs 2A, 2B2	Bank 1 – DIMMs 1A, 1B
MCH	S/R	S/R	S/R
	E	S/R	S/R
	E	E	S/R

	E	D/R	D/R
	E	E	D/R
	D/R	S/R	S/R
	E	D/R	S/R

Table 5: Supported DDR2-400 DIMM Populations

	Bank 3 – DIMMs 3A, 3B	Bank 2 – DIMMs 2A, 2B	Bank 1 – DIMMs 1A, 1B
MCH	S/R	S/R	S/R
	E	S/R	S/R
	E	E	S/R
	E	D/R	D/R
	E	E	D/R
	E	S/R	D/R
	S/R	S/R	D/R

Note: On the Server Board SE7520JR2, when using all dual rank DDR-333 or DDR2-400 DIMMs, a total of four DIMMs can be populated. Configuring more than four dual rank DDR-333 or DDR2-400 DIMMs will result in the BIOS generating a memory configuration error.

Note: Memory between 4GB and 4GB minus 512MB will not be accessible for use by the operating system and may be lost to the user, because this area is reserved for BIOS, APIC configuration space, PCI adapter interface, and virtual video memory space. This means that if 4GB of memory is installed, 3.5GB of this memory is usable. The chipset should allow the remapping of unused memory above the 4GB address, but this memory may not be accessible to an operating system that has a 4GB memory limit.

3.3.3 ECC Memory Initialization

ECC memory must be initialized by the BIOS before it can be used. The BIOS must initialize all memory locations before using them. The BIOS uses the auto-initialize feature of the MCH to initialize ECC. ECC memory initialization cannot be aborted and may result in a noticeable delay in the boot process depending on the amount of memory installed in the system.

3.3.4 Memory Test

System memory is classified as base and extended memory. Base memory is memory that is required for POST. Extended memory is the remaining memory in the system. Extended memory may be contiguous or may have one or more holes. The BIOS memory test accesses all memory except for memory holes.

Memory testing consists of separate base and extended memory tests. The base memory test runs before video is initialized to verify memory required for POST. The BIOS enables video as early as possible during POST to provide a visual indication that the system is functional. At some time after video output has been enabled, BIOS executes the extended memory test. The

status of the extended memory test is displayed on the console. The status of base and extended memory tests are also displayed on an LCD control panel if present.

The extended memory test is configured using the BIOS Setup Utility. The coverage of the test can be configured to one of the following:

- Test every location (Extensive)
- Test one interleave width per kilo-byte of memory (Sparse)
- Test one interleave width per mega-byte of memory (Quick).

The “interleave width” of a memory subsystem is dependent on the chipset configuration. By default, both the base and extended memory tests are configured to the Disabled setting. The extended memory test can be aborted by pressing the <Space> key during the test.

3.3.5 Memory Monitoring

Both the baseboard management controller and BIOS provide support for memory inventory, memory failure LEDs, and failure/state transition events. Memory monitoring features are supported differently depending on which level of server management is used. The following table shows how each feature is supported by management level.

Table 6: Memory Monitoring Support by Server Management Level

Memory Feature	On-board	Professional	Advanced
Inventory	No	Yes	Yes
Correctable Error Reporting	No	Yes	Yes
Uncorrectable Error Reporting	Yes	Yes	Yes

With either Professional or Advanced IMMs installed, the Sahalee BMC maintains one sensor per DIMM. The sensor is IPMI type 21h, Slot/Connector. The Sahalee BMC directly detects the presence or absence of each DIMM and records this in offset 2 of these sensors.

DIMM failure can be detected at BIOS POST or during system operation. POST detected DIMM failures or mis-configuration (incompatible DIMM sizes/speeds/etc) cause the BIOS to disable the failed/affected DIMMs and generate IPMI SEL events, which are sent to the BMC in use.

In addition, using Professional or Advanced IMMs, the BIOS communicates this failure to the Sahalee BMC so that it can be incorporated in the BMC’s DIMM sensor state. DIMM presence and failure states are stored persistently by the Sahalee BMC.

In all management levels, the BIOS is responsible for DIMM FRU LED management and illuminates the LEDs associated with failed or disabled DIMMs.

Correctable memory errors are non-critical errors that do not cause the system to fail. They are detected by the BIOS and are logged as IPMI SEL events when either the Professional or Advanced IMMs are installed. Logging is throttled by error frequency. If more than a certain number of correctable errors occur in an hour, logging is turned off.

Uncorrectable memory errors are critical errors that may cause the system to fail. The BIOS normally detects and logs these errors as IPMI SEL events for all management levels, except in the case described below.

It is possible that a critical hardware error (uncorrectable memory or bus error) may prevent the BIOS from running, reporting the error, and restarting the system. In Professional and Advanced management models, the Sahalee BMC monitors the SMI signal, which, if it stays asserted for a long period of time, is an indication that BIOS cannot run. In this case, the Sahalee BMC logs an SMI Timeout event and probes for errors. If one is found it will log data against the IPMI type 0Ch Memory Sensor and will log against the IPMI 13h Critical Interrupt sensor for a bus error. Both of these can include additional data in bytes 2 and 3 depending on the exact nature of the error and what the chipset reports to the Sahalee BMC.

3.3.6 Memory RASUM Features

The Intel E7520 MCH supports several memory RASUM (Reliability, Availability, Serviceability, Usability, and Manageability) features. These features include the Intel® x4 Single Device Data Correction (x4 SDDC) for memory error detection and correction, Memory Scrubbing, Retry on Correctable Errors, Integrated Memory Initialization, DIMM Sparing, and Memory Mirroring. The following sections describe how each is supported.

Note: The operation of the memory RASUM features listed below is supported regardless of the platform management model used. However, with no Intel® Management Module installed, the system has limited memory monitoring and logging capabilities. It is possible for a RASUM feature to be initiated without notification that the action has occurred when standard Onboard Platform Instrumentation is used.

3.3.6.1 DRAM ECC – Intel® x4 Single Device Data Correction (x4 SDDC)

The DRAM interface uses two different ECC algorithms. The first is a standard SEC/DED ECC across a 64-bit data quantity. The second ECC method is a distributed, 144-bit S4EC-D4ED mechanism, which provides x4 SDDC protection for DIMMS that utilize x4 devices. Bits from x4 parts are presented in an interleaved fashion such that each bit from a particular part is represented in a different ECC word. DIMMs that use x8 devices, can use the same algorithm but will not have x4 SDDC protection, since at most only four bits can be corrected with this method. The algorithm does provide enhanced protection for the x8 parts over a standard SEC-DED implementation. With two memory channels, either ECC method can be utilized with equal performance, although single-channel mode only supports standard SEC/DED.

When memory mirroring is enabled, x4 SDDC ECC is supported in single channel mode when the second channel has been disabled during a fail-down phase. The x4 SDDC ECC is not supported during single-channel operation outside of DIMM mirroring fail-down as it does have significant performance impacts in that environment.

3.3.6.2 Integrated Memory Scrub Engine

The Intel E7520 MCH includes an integrated engine to walk the populated memory space proactively seeking out soft errors in the memory subsystem. In the case of a single bit correctable error, this hardware detects, logs, and corrects the data except when an incoming write to the same memory address is detected. For any uncorrectable errors detected, the scrub

engine logs the failure. Both types of errors may be reported via multiple alternate mechanisms under configuration control. The scrub hardware will also execute “demand scrub” writes when correctable errors are encountered during normal operation (on demand reads, rather than scrub-initiated reads). This functionality provides incremental protection against time-based deterioration of soft memory errors from correctable to uncorrectable.

Using this method, a 16GB system can be completely scrubbed in less than one day. The effect of the scrub writes do not cause any noticeable degradation to memory bandwidth, although they will cause a greater latency for that one very infrequent read that is delayed due to the scrub write cycle.

Note that an uncorrectable error encountered by the memory scrub engine is a “speculative error.” This designation is applied because no system agent has specifically requested use of the corrupt data, and no real error condition exists in the system until that occurs. It is possible that the error resides in an unmodified page of memory that will be simply dropped on a swap back to disk. Were that to occur, the speculative error would simply “vanish” from the system undetected without adverse consequences.

3.3.6.3 Retry on Uncorrectable Error

The Intel E7520 MCH includes specialized hardware to resubmit a memory read request upon detection of an uncorrectable error. When a demand fetch (as opposed to a scrub) of memory encounters an uncorrectable error as determined by the enabled ECC algorithm, the memory control hardware will cause a (single) full resubmission of the entire cache line request from memory to verify the existence of corrupt data. This feature is expected to greatly reduce or eliminate the reporting of false or transient uncorrectable errors in the DRAM array.

Note that any given read request will only be retried a single time on behalf of this error detection mechanism. If the uncorrectable error is repeated, it will be logged and escalated as directed by device configuration. In the memory mirror mode, the retry on an uncorrectable error will be issued to the mirror copy of the target data, rather than back to the devices responsible for the initial error detection. This has the added benefit of making uncorrectable errors in DRAM fully correctable unless the same location in both primary and mirror happens to be corrupt. This RASUM feature may be enabled and disabled via configuration.

3.3.6.4 Integrated Memory Initialization Engine

The Intel E7520 MCH provides hardware managed ECC auto-initialization of all populated DRAM space under software control. Once internal configuration has been updated to reflect the types and sizes of populated DIMM devices, the MCH will traverse the populated address space initializing all locations with good ECC. This not only speeds up the mandatory memory initialization step, but also frees the processor to pursue other machine initialization and configuration tasks.

Additional features have been added to the initialization engine to support high speed population and verification of a programmable memory range with one of four known data patterns (0/F, A/5, 3/C, and 6/9). This function facilitates a limited, very high speed memory test, as well as provides a BIOS accessible memory zeroing capability for use by the operating system.

3.3.6.5 DIMM Sparing Function

To provide a more fault tolerant system, the Intel E7520 MCH includes specialized hardware to support fail-over to a spare DIMM device in the event that a primary DIMM in use exceeds a specified threshold of runtime errors. One of the DIMMs installed per channel, greater than or equal in size than all installed, will not be used but kept in reserve. In the event of significant failures in a particular DIMM, it and its corresponding partner in the other channel (if applicable), will, over time, have its data copied over to the spare DIMM(s) held in reserve. When all the data has been copied, the reserve DIMM(s) will be put into service and the failing DIMM will be removed from service. Only one sparing cycle is supported. If this feature is not enabled, then all DIMMs will be visible in normal address space.

Note: The DIMM Sparing feature requires that the spare DIMM be at least the size of the largest primary DIMM in use.

Hardware additions for this feature include the implementation of tracking register per DIMM to maintain a history of error occurrence, and a programmable register to hold the fail-over error threshold level. The operational model is straightforward: if the fail-over threshold register is set to a non-zero value, the feature is enabled, and if the count of errors on any DIMM exceeds that value, fail-over will commence. The tracking registers themselves are implemented as “leaky buckets,” such that they do not contain an absolute cumulative count of all errors since power-on; rather, they contain an aggregate count of the number of errors received over a running time period. The “drip rate” of the bucket is selectable by software, so it is possible to set the threshold to a value that will never be reached by a “healthy” memory subsystem experiencing the rate of errors expected for the size and type of memory devices in use.

The fail-over mechanism is slightly more complex. Once fail-over has been initiated the MCH must execute every write twice; once to the primary DIMM, and once to the spare. The MCH will also begin tracking the progress of its built-in memory scrub engine. Once the scrub engine has covered every location in the primary DIMM, the duplicate write function will have copied every data location to the spare. At that point, the MCH can switch the spare into primary use, and take the failing DIMM off-line.

Note that this entire mechanism requires no software support once it has been programmed and enabled, until the threshold detection has been triggered to request a data copy. Hardware will detect the threshold initiating fail-over, and escalate the occurrence of that event as directed (signal an SMI, generate an interrupt, or wait to be discovered via polling). Whatever software routine responds to the threshold detection must select a victim DIMM (in case multiple DIMMs have crossed the threshold prior to sparing invocation) and initiate the memory copy. Hardware will automatically isolate the “failed” DIMM once the copy has completed. The data copy is accomplished by address aliasing within the DDR control interface, thus it does not require reprogramming of the DRAM row boundary (DRB) registers, nor does it require notification to the operating system that anything has occurred in memory.

The memory mirroring feature and DIMM sparing are exclusive of each other, only one may be activated during initialization. The selected feature must remain enabled until the next power-cycle. There is no provision in hardware to switch from one feature to the other without rebooting, nor is there a provision to “back out” of a feature once enabled without a full reboot.

3.3.6.6 Memory Mirroring

The memory mirroring feature is fundamentally a way for hardware to maintain two copies of all data in the memory subsystem, such that a hardware failure or uncorrectable error is no longer fatal to the system. When an uncorrectable error is encountered during normal operation, hardware simply retrieves the “mirror” copy of the corrupted data, and no system failure will occur unless both primary and mirror copies of the same data are corrupt simultaneously. Mirroring is supported on dual-channel DIMM populations symmetric both across channels and within each channel. As a result, on the Server Board SE7520JR2 there are two supported configurations for memory mirroring:

- Four DIMM population of completely identical devices (two per channel). Refer to Figure 6, DIMMs labeled 1A, 2A, 1B and 2B must all be identical.

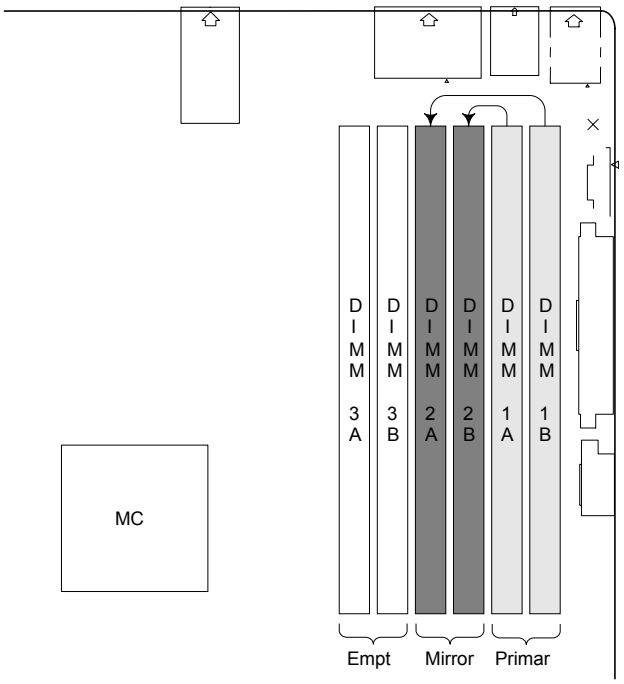


Figure 6. Four DIMM Memory Mirror Configuration

- Six DIMM population with identical devices in slot pairs 1 and 2/3 on each channel. DIMM slots labeled 1A, 1B must be populated with identical dual ranked DIMMs, while DIMMs in the remaining slots must be identical single rank DIMMs. DIMMs between the two groups do not have to be identical. **This configuration is only valid with DDR2 memory**. DDR266/333 mirrored memory configurations are only capable of supporting 2 DIMMs per channel.

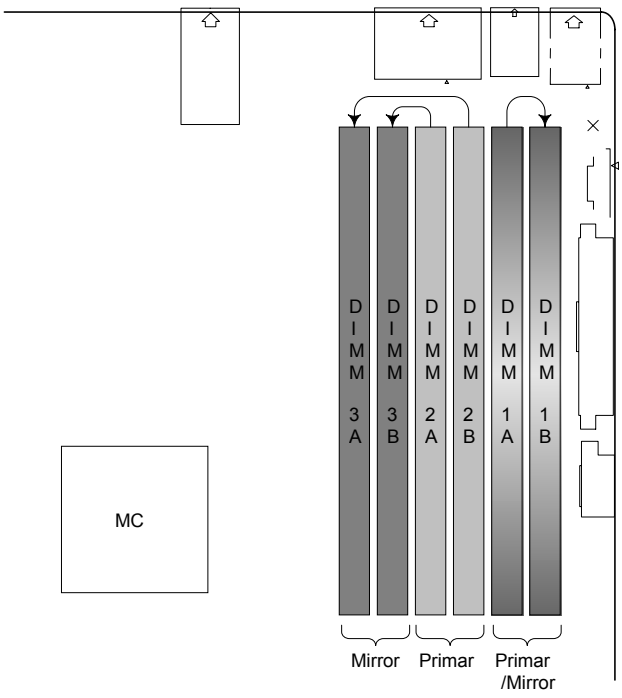


Figure 7. Six DIMM Memory Mirror Configuration (DDR2 Only)

These symmetry requirements are a side effect of the hardware mechanism for maintaining two copies of all main memory data while ensuring that each channel has a full copy of all data in preparation for fail-down to single-channel operation. Every write to memory is issued twice, once to the “primary” location, and again to the “mirror” location, and the data interleaved across the channel pair are swapped for the second write (1A is a copy of 2B, 1B is a copy of 2A etc.). The resulting memory image has two full copies of all data, and a complete copy available on each channel.

Hardware in the MCH tracks which DIMM slots are primaries, and which are mirrors, such that data may be internally realigned to correctly reassemble cache lines regardless of which copy is retrieved. There are four distinct cases for retrieval of the “even” and “odd” chunks of a cache-line of data:

- Interleaved dual-channel read to the primary DIMM with “even” data on channel A
- Interleaved dual-channel read to the mirror DIMM with “even” data on channel B
- Non-interleaved single-channel read pair to channel A with “even” data on the primary DIMM
- Non-interleaved single-channel read pair to channel B with “even” data on the mirror DIMM

When mirroring is enabled via MCH configuration, the memory subsystem maintains two copies of all data as described above, and will retrieve requested data from either primary or mirror based on the state of system address bit 15 (SA[15]). Software may toggle which SA[15] polarity selects primary vs. mirror via a configuration register bit setting. SA[15] was chosen because it is the lowest system address bit that is always used to select the memory row address across all DRAM densities and technologies supported by the E7520 MCH. The toggling of the primary read location based on an address bit will distribute request traffic across

the primary and mirror DIMMs, thereby distributing the thermal image of the workload across all populated DIMM slots, and reducing the chances of thermal-based memory traffic throttling.

In the “Mirrored” operating state, the occurrence of correctable and uncorrectable ECC errors are tracked and logged normally by the MCH, and escalated to system interrupt events as specified by the configuration register settings associated with errors on the memory subsystem. Counters implementing the “leaky bucket” function just described for on-line DIMM sparing track the aggregate count of single-bit and multiple-bit errors on a per DIMM basis.

3.3.6.7 Logging Memory RAS Information to the SEL

In systems configured with either a Professional or Advanced IMM, the system BIOS is responsible for sending the current memory RAS configuration to the Sahalee BMC in accordance with Sahalee BMC spec.

Note: The operation of the memory RASUM features described is supported regardless of the platform management model used. However, with no Intel® Management Module installed, the system has limited memory monitoring and logging capabilities. It is possible for a RASUM feature to be initiated without notification that the action has occurred when using standard on-board platform instrumentation.

BIOS will send the initial memory RAS state during POST memory configuration using the SMS commands. BIOS will update the memory RAS state when memory errors occur that affect the RAS state using the SMM commands.

3.4 I/O Sub-System

The I/O sub-system is made up of several components:

- The MCH provides the PCI-Express interface to the full-height riser slot
- The PXH provides the PCI-X interfaces for the two riser slots, the on-board SCSI controller and on-board Ethernet controllers
- The ICH5-R provides the interface for the onboard video controller, super IO chip, and management sub-system.

This section describes the function of each I/O interface and how they operate on the Server Board SE7520JR2.

3.4.1 PCI Subsystem

The primary I/O interface for the Server Board SE7520JR2 is PCI, with four independent PCI bus segments.

- A PCI 33MHz/32-bit bus segment (P32-A) is controlled through the ICH5-R.
- Two PCI-X 100MHz/64-bit bus segments (P64-A and P64-B) are controlled through PXH PCI bridge.
- One dual x4 PCI-Express (P64-Express) bus segment is controlled from the MCH.

The table below lists the characteristics of the four PCI bus segments.

Table 7: PCI Bus Segment Characteristics

PCI Bus Segment	Voltage	Width	Speed	Type	PCI I/O Card Slots
P32-A	5 V	32-bits	33 MHz	PCI	None. Internal component use only
P64-A	3.3 V	64-bits	100 MHz	PCI-X	Common riser slot capable of supporting full-length PCI-X or PCI-E add-in cards
P64-B	3.3 V	64-bits	100 MHz	PCI-X	One riser slot supporting only low-profile add-in cards
P64-Express	Differential	64-bits	Dual x4	PCI-E	Common riser slot capable of supporting full-length PCI-X or PCI-E add-in cards

3.4.1.1 P32-A: 32-bit, 33-MHz PCI Subsystem

All 32-bit, 33-MHz PCI I/O is directed through the ICH5-R. The 32-bit, 33-MHz PCI segment provided by the ICH5-R is known as the P32-A segment. The P32-A segment supports the following embedded devices:

- 2D/3D Graphics Accelerator: ATI Rage XL Video Controller
- SIO Chip: National Semiconductor* PC87417 Super I/O
- Hardware monitoring sub-system: SMBUS

3.4.1.2 P64-A and P64-B: 64-bit, 100MHz PCI Subsystem

Two peer 64-bit PCI-X bus segments are directed through the PXH PCI Bridge. The first PCI-X segment, P64-A, supports the interface for the on-board LSI* 53C1030 Ultra320 SCSI controller, in addition to supporting up to three PCI-X add-in cards from the full-height PCI riser slot. The second PCI-X segment, P64-B, supports the interface to the on-board Intel® 82546GB dual port Gigabit network controller, in addition to up to three PCI-X add-in cards from the low profile PCI riser slot.

3.4.1.3 P64-Express: Dual x4 PCI Bus Segment

The full height riser slot supports both X4 and X8 PCI-E type widths. In a 2U system, the baseboard supports two x4 PCI-E slots. In a 1U system, the baseboard supports one x8 PCI-E slot.

The BIOS performs link training with PCI-E devices during boot and checks the resulting status. If it detects that a port is not connected to a PCI-E device, it disables the port.

3.4.1.4 PCI Riser Slots

The Server Board SE7520JR2 has two riser slots capable of supporting riser cards for both 1U and 2U system configurations. Because of board placement resulting in different pin orientations, and expanded technology support associated with the full-height riser, the riser slots are proprietary and require different riser cards.

The low profile riser slot (J5F1) utilizes a 202-pin connector. It is capable of supporting up to three low profile PCI-X add-in cards, depending on the riser card used. The P64-B bus can support bus speeds of up to 100MHz with up to two PCI-X 100MHz cards installed. The bus speed will drop to 66MHz when three PCI-X 100MHz cards are installed, or will match the card speed of the lowest speed card on the bus. Ie) If any of the add-cards installed on the P64B bus

supports a maximum of 66MHz, the entire bus will throttle down to 66MHz to match the supported frequency of that card. When populating add-in cards, the add-in cards must be installed starting with the slot furthest from the baseboard. Ie) When using a three slot riser, a single PCI-X add-in card must be installed in the top PCI slot. A second add-in card must be installed in the middle slot, and so on. These population rules must be followed to maintain the signal integrity of the bus.

The full-height riser slot implements Intel® Adaptive Slot Technology. This 280-pin connector is capable of supporting riser cards that meet either the PCI-X or PCI-Express technology specifications. As a PCI-X only bus, using a baseboard with integrated SCSI and passive riser card, the P64-A bus can support bus speeds of up to 100MHz with up to two PCI-X 100MHz cards installed. The bus speed will drop to 66MHz when three PCI-X 100MHz cards are installed, or will match the card speed of the lowest speed card on the bus. Ie) If any of the add-cards installed on the P64A bus supports a maximum of 66MHz, the entire bus will throttle down to 66MHz to match the supported frequency of that card. When populating add-in cards, the add-in cards must be installed starting with the slot furthest from the baseboard. Ie) When using a three slot passive riser, a single PCI-X add-in card must be installed in the top PCI slot. A second add-in card must be installed in the middle slot, and so on. These population rules must be followed to maintain the signal integrity of the bus. On a baseboard with no integrated SCSI, the P64-A bus is capable of supporting a bus speed of up to 133MHz when a 1U, single slot riser card is used. I

Intel also makes available an active three slot PCI-X riser which utilizes a separate on board PXH chip. This riser is capable of supporting up to two PCI-X 133MHz cards in addition to a third PCI-X 100MHz card. If used in a baseboard with no on-board SCSI controller, the third add-in slot can also operate at 133MHz.

When configured with a riser card supporting PCI-Express technology, the full height riser slot can support riser cards that have either one x 8 PCI-Express card, or two x 4 PCI-Express cards. Intel makes available a 1U single slot x8 riser card and a 2U three slot riser card which provides two x8 connectors each supporting x4 data widths. The third slot is a PCI-X slot. Using a baseboard configured with an integrated SCSI controller, the PCI-X add-in slot is capable of supporting a bus speed of up to 100MHz. Installed in a baseboard with no integrated SCSI controller, this PCI-X add-in slot is capable of supporting a bus speed of up to 133MHz.

3.4.1.5 PCI Scan Order

The BIOS assigns PCI bus numbers in a depth-first hierarchy, in accordance with the *PCI Local Bus Specification*. When a bridge device is located, the bus number is incremented in exception of a bridge device in the chipsets. Scanning continues on the secondary side of the bridge until all subordinate buses are defined. PCI bus numbers may change when PCI-PCI bridges are added or removed. If a bridge is inserted in a PCI bus, all subsequent PCI bus numbers below the current bus are increased by one.

3.4.1.6 PCI Bus Numbering

PCI configuration space protocol requires that all PCI buses in a system be assigned a bus number. Bus numbers must be assigned in ascending order within hierarchical buses. Each PCI bridge has registers containing its PCI bus number and subordinate PCI bus number, which must be loaded by POST code. The subordinate PCI bus number is the bus number of the last

hierarchical PCI bus under the current bridge. The PCI bus number and the subordinate PCI bus number are the same in the last hierarchical bridge.

3.4.1.7 Device Number and IDSEL Mapping

Each device under a PCI bridge has its IDSEL input connected to one bit out of the PCI bus address/data signals AD[31::11] for the PCI bus. Each IDSEL-mapped AD bit acts as a chip select for each device on PCI. The host bridge responds to a unique PCI device ID value that, along with the bus number, cause the assertion of IDSEL for a particular device during configuration cycles. The following table shows the correspondence between IDSEL values and PCI device numbers for the PCI bus. The lower five bits of the device number are used in CONFIG_ADDRESS bits [15::11].

Table 8: PCI Configuration IDs and Device Numbers

PCI Device	IDSEL	Bus# / Device# / Function#
MCH host-HI bridge/DRAM controller		00 / 00 / 0
MCH DRAM Controller Error Reporting		00/00/1
MCH DMA controller		00/01/00
MCH EXP Bridge A0		00/02/00
MCH EXP Bridge A1		00/03/00
MCH EXP Bridge B0		00/04/00
MCH EXP Bridge B1		00/05/00
MCH EXP Bridge C0		00/06/00
MCH EXP Bridge C1		00/07/00
MCH Extended Configuration		00/08/00
ICH5R Hub interface to PCI bridge		00 / 30 / 00
ICH5R PCI to LPC interface		00 / 31 / 00
ICH5R IDE controller		00 / 31 / 01
ICH5R Serial ATA		00 / 31 / 02
ICH5R SMBus controller		00 / 31 / 03
ICH5R USB UHCI controller #1		00 / 29 / 00
ICH5R USB UHCI controller #2		00 / 29 / 01
ICH5R USB UHCI controller #3		00 / 29 / 02
ICH5R USB 2.0 EHCI controller		00 / 29 / 07
FL Slot1 (64-bit, PCIX-100)	P1A_AD17	/ 01 /
FL Slot2(64-bit, PCI-X-100)	P1A_AD18	/ 02 /
FL Slot3 (64-bit, PCI-X-100)	P1A_AD19	/ 03 /
FL PXH Slot1	P2A_AD17	/01/
FL PXH Slot 2	P2B_AD17	/01/
FL PCI-E x8 Slot1		/00/
FL PCI-E x4 Slot1		/00/
FL PCI-E x4 Slot2		/00/
LP Slot1 (64-bit, PCI-X-100)	P1B_AD17	/ 01 /
LP Slot2 (64-bit, PCI-X-100)	P1B_AD18	/ 02 /
LF Slot3 (64-bit, PCI-X-100)	P1B_AD19	/ 03 /
On board device		
Intel 82546GB(1Gb) NIC w/ dual channel	P1B_AD20	/ 04 /0,1
LSI53C1030 Ultra 320 SCSI w/ dual channel	P1A_AD21	/05/0,1
ATI Rage XL (PCI VGA)	PC_AD28	/ 12 /0

Note: Bus Numbers may change depending on the type of riser card used.

3.4.1.8 Resource Assignment

The resource manager assigns the PIC-mode interrupt for the devices that will be accessed by the legacy code. The BIOS configures the PCI Base Address Registers (BAR) and the command register of each device. Software must not make assumptions about the scan order of devices or the order in which resources are allocated to them. The BIOS supports the INT 1Ah PCI BIOS interface calls.

3.4.1.9 Automatic IRQ Assignment

The BIOS automatically assigns IRQs to devices in the system for legacy compatibility. No method is provided to manually configure the IRQs for devices.

3.4.1.10 Option ROM Support

The BIOS dispatches the option ROMs to available memory space in the address range 0c0000h-0e7fffh. Given the limited space for option ROMs, the BIOS allows for disabling of legacy ROM posting via the BIOS Setup. Onboard and per-slot option ROM disable options are also available in BIOS Setup. The option to disable the onboard video option ROM is not available.

The option ROM space is also used by the console redirection binary (if enabled) and the user binary (if present and configured for runtime usage).

The SE7520JR2 BIOS integrates option ROMs for the Intel® 82546GB, the ATI* Rage XL, and the LSI* 53C1030 SCSI controller.

3.4.1.11 PCI APIs

The system BIOS supports the INT 1Ah, AH = B1h functions as defined in the PCI BIOS Specification. The system BIOS supports the real mode interfaces and does not support the protected mode interfaces.

3.4.2 Split Option ROM

The BIOS supports the split option ROM algorithm per the PCI 3.0 specification.

3.4.3 Interrupt Routing

The Server Board SE7520JR2 interrupt architecture accommodates both PC-compatible PIC mode and APIC mode interrupts through use of the integrated I/O APICs in the ICH5-R.

3.4.3.1 Legacy Interrupt Routing

For PC-compatible mode, the ICH5-R provides two 82C59-compatible interrupt controllers. The two controllers are cascaded with interrupt levels 8-15 entering on level 2 of the primary interrupt controller (standard PC configuration). A single interrupt signal is presented to the processors, to which only one processor will respond for servicing. The ICH5-R contains configuration registers that define which interrupt source logically maps to I/O APIC INTx pins.

Both PCI and IRQ types of interrupts are handled by the ICH5-R. The ICH5-R translates these to the APIC bus. The numbers in the table below indicate the ICH5-R PCI interrupt input pin to which the associated device interrupt (INTA, INTB, INTC, INTD) is connected. The ICH5-R I/O APIC exists on the I/O APIC bus with the processors.

Table 9: PCI Interrupt Routing/Sharing

Interrupt	INT A	INT B	INT C	INT D
Video	ICH5R_PIRQB			
IDE RAID	ICH5R_PIRQC			
NIC 10/100 (Not used on SE7520JR2)	ICH5R_PIRQD			
SIO	ICH5R_SERIRQ			
Legacy IDE	ICH5R_PIRQ14			
Legacy IDE	ICH5R_PIRQ15			
82546GB #1	P64A_IRQ6			
82546GB #2	P64A_IRQ7			
SCSI Controller #1	P64B_IRQ2			
SCSI Controller #2	P64B_IRQ1			
FL Riser TCK & TCO	P64A_IRQ0	P64A_IRQ3	P64A_IRQ5	P64A_IRQ4
P64-A Slot 1	P64A_IRQ0	P64A_IRQ3	P64A_IRQ5	P64A_IRQ4
P64-A Slot 2	P64A_IRQ3	P64A_IRQ5	P64A_IRQ4	P64A_IRQ0
P64-A Slot 3	P64A_IRQ5	P64A_IRQ4	P64A_IRQ2	P64A_IRQ1
LP Riser	P64B_IRQ4	P64B_IRQ3	P64B_IRQ2	P64B_IRQ1
P64-B Slot 1	P64B_IRQ4	P64B_IRQ3	P64B_IRQ2	P64B_IRQ1
P64-B Slot 2	P64B_IRQ3	P64B_IRQ2	P64B_IRQ1	P64B_IRQ4
P64-B Slot 3	P64B_IRQ2	P64B_IRQ1	P64B_IRQ4	P64B_IRQ3

3.4.3.2 APIC Interrupt Routing

For APIC mode, the Server Board SE7520JR2 interrupt architecture incorporates three Intel I/O APIC devices to manage and broadcast interrupts to local APICs in each processor. The Intel I/O APICs monitor each interrupt on each PCI device including PCI slots in addition to the ISA compatibility interrupts IRQ(0-15). When an interrupt occurs, a message corresponding to the interrupt is sent across a three-wire serial interface to the local APICs. The APIC bus minimizes interrupt latency time for compatibility interrupt sources. The I/O APICs can also supply greater than 16 interrupt levels to the processor(s). This APIC bus consists of an APIC clock and two bidirectional data lines.

3.4.3.3 Legacy Interrupt Sources

The table below recommends the logical interrupt mapping of interrupt sources on the Server Board SE7520JR2. The actual interrupt map is defined using configuration registers in the ICH5-R.

Table 10: Interrupt Definitions

ISA Interrupt	Description
IRQ0	Timer/counter, HPET #0 in legacy replacement Mode. In APIC mode, cascade from 8259 controller #1
IRQ1	Keyboard
IRQ2	Slave controller INTR output. In APIC mode timer/counter, HPET#0
IRQ3	Serial port A
IRQ4	Serial port B
IRQ5	Parallel Port (Not implemented)
IRQ6	Floppy
IRQ7	Parallel port, generic (Not implemented)
IRQ8	RTC/HPET#1 in legacy replacement mode
IRQ9	Generic, Option for SCI
IRQ10	Generic, Option for SCI
IRQ11	HPET#2, option for SCSI, TCO*
IRQ12	PS2 Mouse
IRQ13	FERR
IRQ14	Primary ATA, legacy mode
IRQ15	Secondary ATA, legacy mode
PIRQA	USB 2.0 Controller #1 and #4
PIRQB	Video
PIRQC	USB 2.0 Controller #3, Native IDE, S-ATA
PIRQD	USB 2.0 Controller #2
PIRQE	Option for SCI, TCO, HPET#0,1,2
PIRQF	Option for SCI, TCO, HPET#0,1,2
PIRQG	Option for SCI, TCO, HPET#0,1,2
PIRQH	USB 2.0 EHCI controller #1, option for SCI, TCO, HPET#0,1,2
Ser IRQ	SIO3

3.4.3.4 Serialized IRQ Support

The Server Board SE7520JR2 supports a serialized interrupt delivery mechanism. Serialized Interrupt Requests (SERIRQ) consists of a start frame, a minimum of 17 IRQ / data channels, and a stop frame. Any slave device in quiet mode may initiate the start frame. While in continuous mode, the start frame is initiated by the host controller.

3.4.3.5 IRQ Scan for PCIIRQ

The IRQ / data frame structure includes the ability to handle up to 32 sampling channels with the standard implementation using the minimum 17 sampling channels. The Server Board SE7520JR2 has an external PCI interrupt serializer for PCIIRQ scan mechanism of ICH5-R to support 16 PCIIRQs.

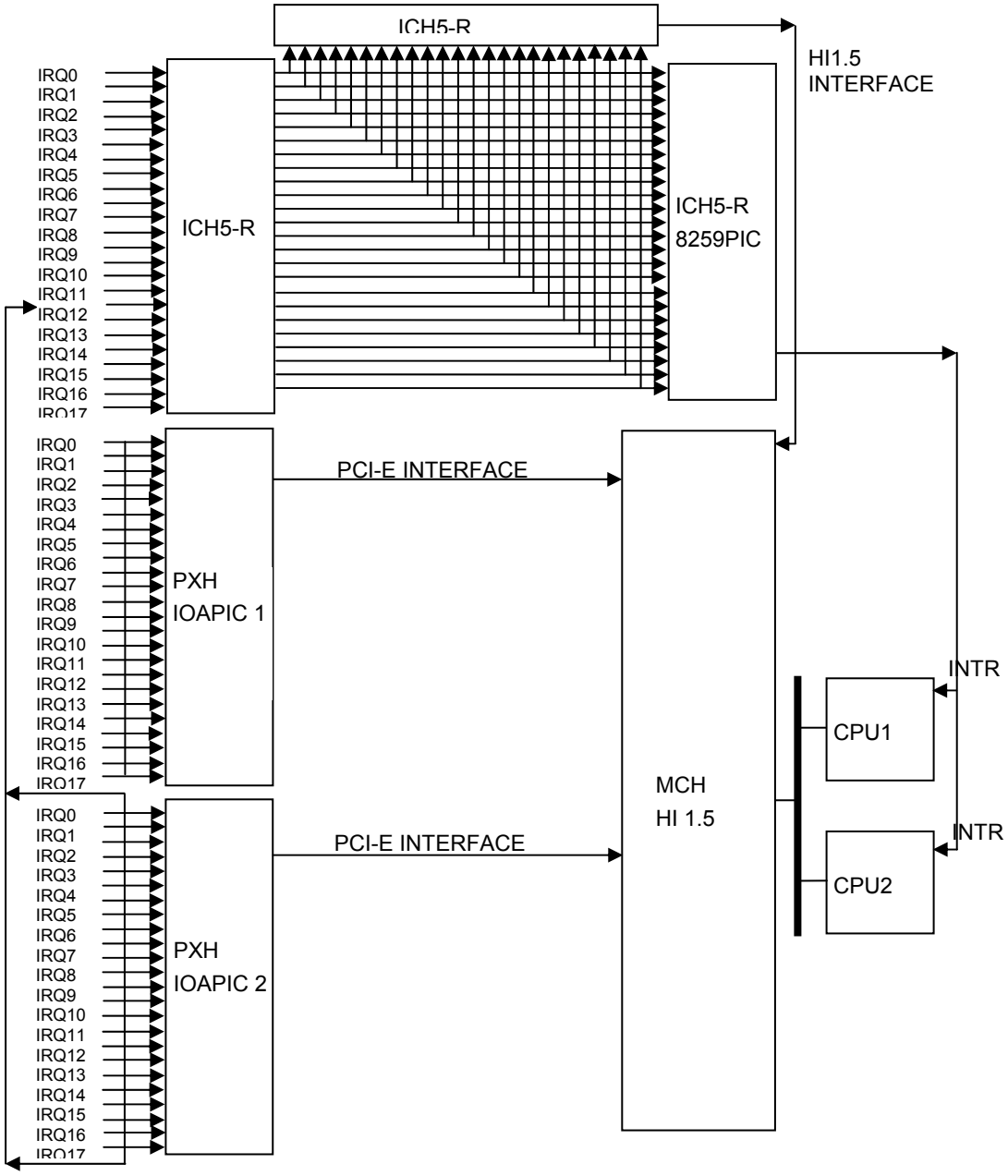


Figure 8. Interrupt Routing Diagram (ICH5-R Internal)

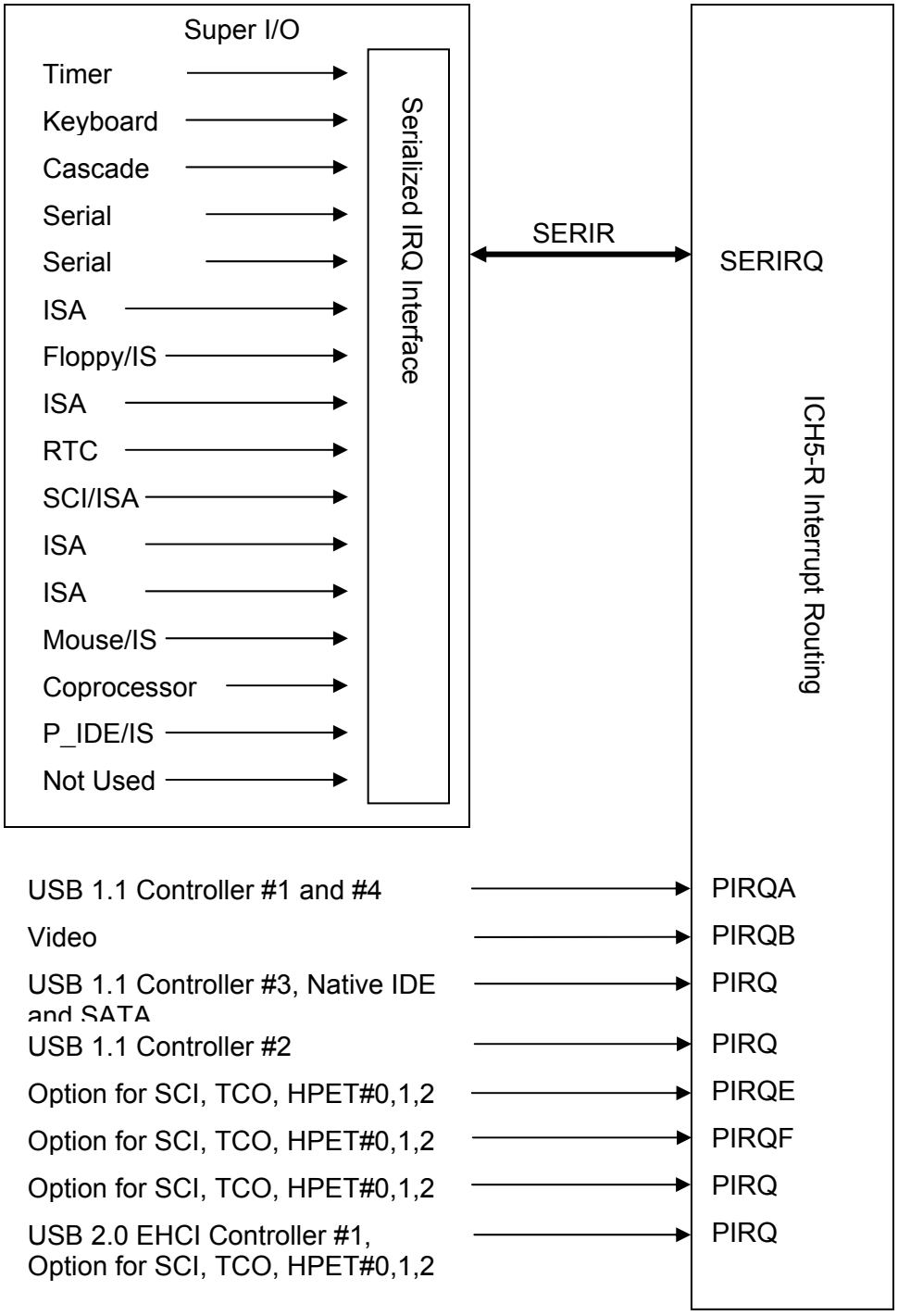


Figure 9. Interrupt Routing Diagram

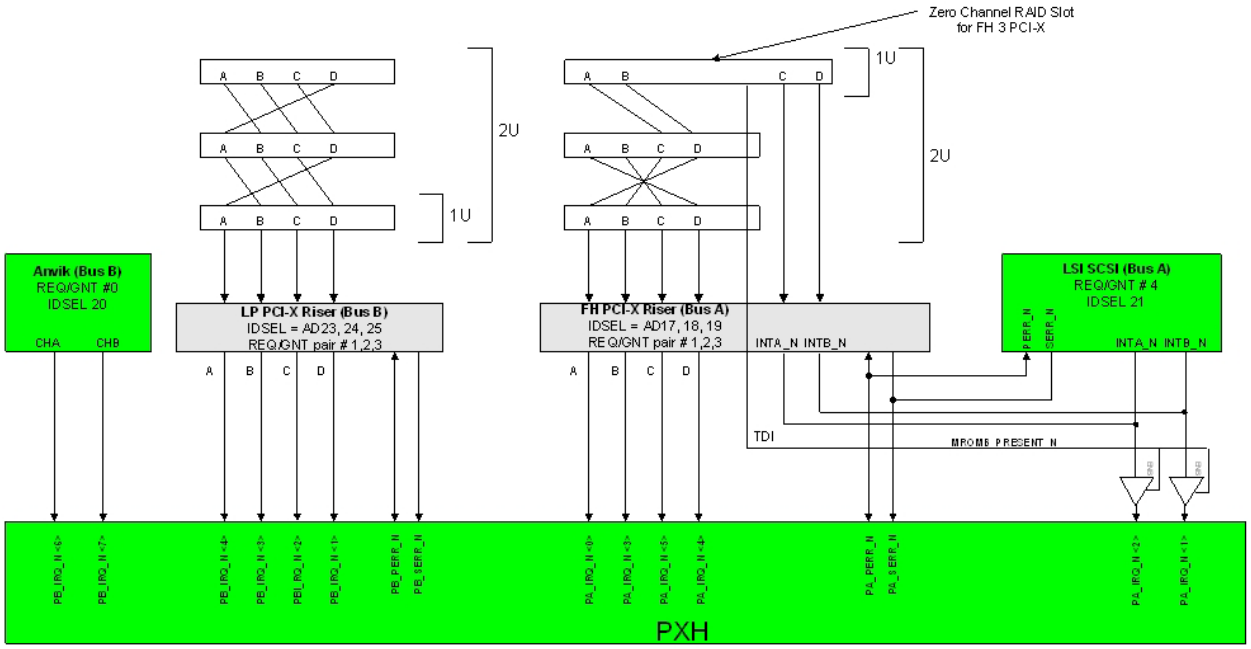


Figure 10. PCI Interrupt Mapping Diagram

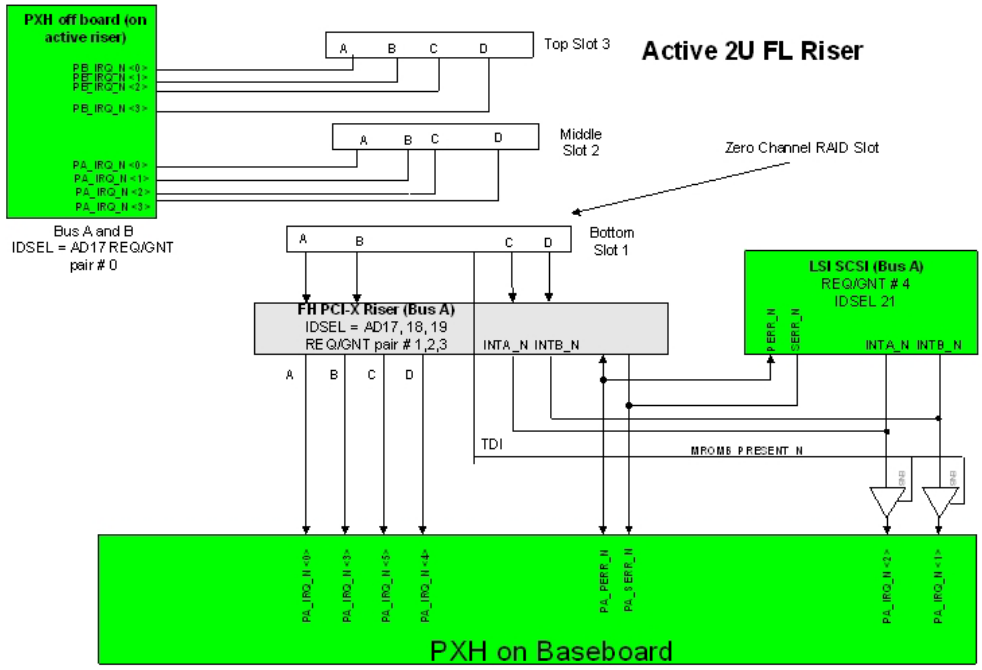


Figure 11. PCI Interrupt Mapping Diagram for 2U Active Riser Card

3.4.4 SCSI Support

The SCSI sub-system consists of the LSI 53C1030 Dual Channel Ultra320 SCSI controller, one internal 80-pin connector (SCSI Channel A), one external high 80-pin density SCSI connector (SCSI channel B), and on-board termination for both SCSI channels.

3.4.4.1 LSI* 53C1030 Dual Channel Ultra320 SCSI Controller

The LSI53C1030 is a PCI-X to Dual Channel Ultra320 SCSI Multifunction Controller that supports the PCI Local Bus Specification, Revision 2.2, and the PCI-X Addendum to the PCI Local Bus Specification, Revision 1.0a.

The LSI53C1030 supports up to a 64-bit, 133 MHz PCI-X bus. DT clocking enables the LSI53C1030 to achieve data transfer rates of up to 320 megabytes per second (MB/s) on each SCSI channel, for a total bandwidth of 640 MB/s on both SCSI channels.

SureLINK* Domain Validation detects the SCSI bus configuration and adjusts the SCSI transfer rate to optimize bus interoperability and SCSI data transfer rates. SureLINK Domain Validation provides three levels of domain validation, assuring robust system operation.

The LSI53C1030 integrates two high-performance SCSI Ultra320 cores and a 64-bit, 133 MHz PCI-X bus master DMA core. The LSI53C1030 employs three ARM* ARM966E-S processors to meet the data transfer flexibility requirements of the Ultra320 SCSI, PCI, and PCI-X specifications. Separate ARM processors support each SCSI channel and the PCI/PCI-X interface.

These processors implement the LSI* Logic Fusion-MPT* architecture, a multithreaded I/O algorithm that supports data transfers between the host system and SCSI devices with minimal host processor intervention. Fusion-MPT technology provides an efficient architecture that solves the protocol overhead problems of previous intelligent and non-intelligent adapter designs. LVDlink* technology is the LSI Logic implementation of Low Voltage Differential (LVD) SCSI. LVDlink transceivers allow the LSI53C1030 to perform either Single-Ended (SE) or LVD transfers.

The LSI* 53C1030 SCSI controller implements a regular SCSI solution or a RAID On MotherBoard (ROMB) solution. This RAID functionality is included in the LSI option rom and allows the user to select either Integrated Mirroring (IME) or Integrated Striping (IS) RAID mode. The system BIOS provides a setup option to allow the user to select one of these two modes

The LSI Logic BIOS Configuration Utility or the IM DOS Configuration Utility is used to configure the IME and IS firmware attributes. Using the LSI Logic BIOS and drivers adds support of physical device recognition for the purpose of Domain Validation and Ultra320 SCSI expander configuration. Host-based status software monitors the state of the mirrored drives and reports error conditions as they arise.

3.4.4.1.1 53C1030 Summary of Features

The Ultra320 SCSI features for the LSI53C1030 include:

- Double transition (DT) clocking
- Packetized protocol
- Paced transfers

- Quick arbitrate and select (QAS)
- Skew compensation
- Inter-symbol interference (ISI) compensation
- Cyclic redundancy check (CRC)
- Domain validation technology

The LSI53C1030 contains the following SCSI performance features:

- Supports Ultra320 SCSI
- Paced transfers using a free running clock
- 320 MB/s data transfer rate on each SCSI channel
- Mandatory packetized protocol
- Quick arbitrate and select (QAS)
- Skew compensation with bus training
- Transmitter precompensation to overcome ISI effects for SCSI data signals
- Retained training information (RTI)
- Offers a performance optimized architecture
- Three ARM966E-S processors provide high performance with low latency
- Two independent Ultra320 SCSI channels
- Designed for optimal packetized performance
- Uses proven integrated LVDlink transceivers for direct attach to either LVD or SE SCSI buses with precision-controlled slew rates
- Supports expander communication protocol (ECP)
- Uses the Fusion-MPT (Message Passing Technology) drivers to provide support for Windows*, Linux, and NetWare* operating systems

The LSI53C1039 has a 133 MHz, 64-bit PCI/PCI-X interface that supports the following PCI features:

- Operates at 33 MHz or 66 MHz PCI
- Operates at up to 133 MHz PCI-X
- Supports 32-bit or 64-bit data
- Supports 32-bit or 64-bit addressing through Dual Address Cycles (DAC)
- Provides a theoretical 1066 Mbytes/s zero wait state transfer rate
- Complies with the PCI Local Bus Specification, Revision 2.2
- Complies with the PCI-X Addendum to the PCI Local Bus Specification, Revision 1.0a
- Complies with the PCI Power Management Interface Specification, Revision 1.1
- Complies with the PC2001 System Design Guide
- Offers unmatched performance through the Fusion-MPT architecture
- Provides high throughput and low CPU utilization to off load the host processor
- Presents a single electrical load to the PCI Bus (True PCI Multifunction Device)
- Uses SCSI Interrupt Steering Logic (SISL) to provide alternate interrupt routing for RAID applications

- Reduces Interrupt Service Routine (ISR) overhead with interrupt coalescing
- Supports 32-bit or 64-bit data bursts with variable burst lengths
- Supports the PCI Cache Line Size register
- Supports the PCI Memory Write and Invalidate, Memory Read Line, and Memory Read Multiple commands
- Supports the PCI-X Memory Read Dword, Split Completion, Memory Read Block, and Memory Write Block commands
- Supports up to 8 PCI-X outstanding split transactions

- Supports Message Signaled Interrupts (MSI)

3.4.4.2 Zero Channel RAID

The Server Board SE7520JR2 has support for Zero Channel RAID (ZCR) which follows the RUBI2 standard. It will not have support for zero channel RAID cards that follow the RADIOS standard. See the SE7520JR2 Tested Hardware and OS list for a list of supported ZCR cards.

Zero channel RAID (ZCR) capabilities enable the LSI 53C1030 to respond to accesses from a PCI RAID controller card or chip that is able to generate ZCR cycles. The LSI53C1030's ZCR functionality is controlled through the ZCR_EN/ and the IOPD_GNT/ signals. Both of these signals have internal pull-ups and are active LOW. The ZCR_EN/ signal enables ZCR support on the LSI53C1030. Pulling ZCR_EN/ LOW enables ZCR operation. When ZCR is enabled, the LSI53C1030 responds to PCI configuration cycles when the IOPD_GNT/ and IDSEL signal are asserted. Pulling ZCR_EN/ HIGH disables ZCR support on the LSI53C1030 and causes the LSI53C1030 to behave as a normal PCI-X to Ultra320 SCSI controller. When ZCR is disabled, the IOPD_GNT/ signal has no effect on the LSI53C1030 operation. The IOPD_GNT/ pin on the LSI53C1030 should be connected to the PCI GNT/ signal of the external I/O processor. This allows the I/O processor to perform PCI configuration cycles to the LSI53C1030 when the I/O processor is granted the PCI bus. This configuration also prevents the system processor from accessing the LSI53C1030 PCI configuration registers.

On the Server Board SE7520JR2, a ZCR card is only supported on the full-height riser slot. When installing the card, it MUST be populated in the PCI-X add-in slot furthest from the baseboard. No other add-in card slot has support for a ZCR card.

3.4.5 IDE Support

Integrated IDE controllers of the ICH5-R provide two independent IDE channels. Each is capable of supporting up to two devices. A standard 40-pin IDE connector on the baseboard interfaces with one channel. The signals of the second IDE channel are routed to the high-density 100-pin backplane connector for use in either the Intel® Server Chassis SR1400 (1U chassis) or the Intel Server Chassis SR2400 (2U chassis). Both IDE channels can be configured and enabled or disabled by accessing the BIOS Setup Utility during POST.

The BIOS supports the ATA/ATAPI Specification, version 6. It initializes the embedded IDE controller in the chipset south-bridge and the IDE devices that are connected to these devices. The BIOS scans the IDE devices and programs the controller and the devices with their optimum timings. The IDE disk read/write services that are provided by the BIOS use PIO mode, but the BIOS will program the necessary Ultra DMA registers in the IDE controller so that the operating system can use the Ultra DMA Modes.

The BIOS initializes and supports ATAPI devices such as LS-120/240, CDROM, CD-RW and DVD.

The BIOS initializes and supports S-ATA devices just like P-ATA devices. It initializes the embedded the IDE controllers in the chipset and any S-ATA devices that are connected to these controllers. From a software standpoint, S-ATA controllers present the same register interface as the P-ATA controllers. Hot plugging of S-ATA drives during the boot process is not supported by the BIOS and may result in undefined behavior.

3.4.5.1 Ultra ATA/100

The IDE interfaces of the ICH5R DMA protocol redefines signals on the IDE cable to allow both host and target throttling of data and transfer rates of up to 100MB/s.

3.4.5.2 IDE Initialization

The BIOS supports the ATA/ATAPI Specification, version 6 or later. The BIOS initializes the embedded IDE controller in the chipset (ICH5-R) and the IDE devices that are connected to these devices. The BIOS scans the IDE devices and programs the controller and the devices with their optimum timings. The IDE disk read/write services that are provided by the BIOS use PIO mode, but the BIOS programs the necessary Ultra DMA registers in the IDE controller so that the operating system can use the Ultra DMA Modes.

3.4.6 SATA Support

The integrated Serial ATA (SATA) controller of the ICH5-R provides two SATA ports on the baseboard. The SATA ports can be enabled/disabled and/or configured by accessing the BIOS Setup Utility during POST.

The SATA function in the ICH5-R has dual modes of operation to support different operating system conditions. In the case of native IDE-enabled operating systems, the ICH5-R has separate PCI functions for serial and parallel ATA. To support legacy operating systems, there is only one PCI function for both the serial and parallel ATA ports. The MAP register provides the ability to share PCI functions. When sharing is enabled, all decode of I/O is done through the SATA registers. A software write to the Function Disable Register (D31, F0, offset F2h, bit 1) causes Device 31, Function 1 (IDE controller) to hidden, and its configuration registers are not used. The SATA Capability Pointer Register (offset 34h) will change to indicate that MSI is not supported in combined mode.

The ICH5-R SATA controller features two sets of interface signals that can be independently enabled or disabled. Each interface is supported by an independent DMA controller. The ICH5-R SATA controller interacts with an attached mass storage device through a register interface that is equivalent to that presented by a traditional IDE host adapter. The host software follows existing standards and conventions when accessing the register interface and follows standard command protocol conventions.

SATA interface transfer rates are independent of UDMA mode settings. SATA interface transfer rates will operate at the bus's maximum speed, regardless of the UDMA mode reported by the SATA device or the system BIOS.

3.4.6.1 SATA RAID

The Intel® RAID Technology solution, available with the 82801ER ICH5 R (ICH5R), offers data striping for higher performance (RAID Level 0), alleviating disk bottlenecks by taking advantage of the dual independent SATA controllers integrated in the ICH5R. There is no loss of PCI resources (request/grant pair) or add-in card slot.

Intel RAID Technology functionality requires the following items:

- ICH5-R
- Intel RAID Technology Option ROM must be on the platform
- Intel® Application Accelerator RAID Edition drivers, most recent revision
- Two SATA hard disk drives

Intel RAID Technology is not available in the following configurations:

- The SATA controller in compatible mode
- Intel RAID Technology has been disabled

3.4.6.2 Intel® RAID Technology Option ROM

The Intel RAID Technology for SATA Option ROM provides a pre-OS user interface for the Intel RAID Technology implementation and provides the ability for an Intel RAID Technology volume to be used as a boot disk as well as to detect any faults in the Intel RAID Technology volume(s) attached to the Intel RAID controller.

3.4.7 Video Support

The Server Board SE7520JR2 provides an ATI* Rage XL PCI graphics accelerator, along with 8 MB of video SDRAM and support circuitry for an embedded SVGA video subsystem. The ATI Rage XL chip contains a SVGA video controller, clock generator, 2D and 3D engine, and RAMDAC in a 272-pin PBGA. One 2Mx32 SDRAM chip provides 8 MB of video memory.

The SVGA subsystem supports a variety of modes, up to 1600 x 1200 resolution in 8/16/24/32 bpp modes under 2D, and up to 1024 x 768 resolution in 8/16/24/32 bpp modes under 3D. It also supports both CRT and LCD monitors up to 100 Hz vertical refresh rate.

Video is accessed using a standard 15-pin VGA connector found on the back edge of the server board. Video signals are also made available through either of two control panel connectors allowing for an optional video connector to be present on the platform's control panel. Video is routed to the rear video connector by default. Circuitry on the baseboard disables the rear video connector when a monitor is plugged in to the control panel video connector. "Hot plugging" the video while the system is still running, is supported.

On-board video can be disabled using the BIOS Setup Utility or when an add-in video card is installed. System BIOS also provides the option for dual video operation when an add-in video card is configured in the system.

3.4.7.1 Video Modes

The Rage XL chip supports all standard IBM VGA modes. The following table shows the 2D/3D modes supported for both CRT and LCD.

Table 11: Video Modes

2D Mode	Refresh Rate (Hz)	2D Video Mode Support			
		8 bpp	16 bpp	24 bpp	32 bpp
640x480	60, 72, 75, 90, 100	Supported	Supported	Supported	Supported
800x600	60, 70, 75, 90, 100	Supported	Supported	Supported	Supported
1024x768	60, 72, 75, 90, 100	Supported	Supported	Supported	Supported
1280x1024	43, 60	Supported	Supported	Supported	Supported
1280x1024	70, 72	Supported	–	Supported	Supported
1600x1200	60, 66	Supported	Supported	Supported	Supported
1600x1200	76, 85	Supported	Supported	Supported	–
3D Mode	**Refresh Rate (Hz)**	**3D Video Mode Support with Z Buffer Enabled**			
		8 bpp	**16 bpp**	**24 bpp**	**32 bpp**
640x480	60,72,75,90,100	Supported	Supported	Supported	Supported
800x600	60,70,75,90,100	Supported	Supported	Supported	Supported
1024x768	60,72,75,90,100	Supported	Supported	Supported	Supported
1280x1024	43,60,70,72	Supported	Supported	–	–
1600x1200	60,66,76,85	Supported	–	–	–
3D Mode	**Refresh Rate (Hz)**	**3D Video Mode Support with Z Buffer Disabled**			
		8 bpp	**16 bpp**	**24 bpp**	**32 bpp**
640x480	60,72,75,90,100	Supported	Supported	Supported	Supported
800x600	60,70,75,90,100	Supported	Supported	Supported	Supported
1024x768	60,72,75,90,100	Supported	Supported	Supported	Supported
1280x1024	43,60,70,72	Supported	Supported	Supported	–
1600x1200	60,66,76,85	Supported	Supported	–	–

3.4.7.2 Video Memory Interface

The memory controller subsystem of the Rage XL arbitrates requests from direct memory interface, the VGA graphics controller, the drawing coprocessor, the display controller, the video scalar, and hardware cursor. Requests are serviced in a manner that ensures display integrity and maximum CPU/coprocessor drawing performance.

The Server Board SE7520JR2 supports an 8MB (512Kx32bitx4 Banks) SDRAM device for video memory. The following table shows the video memory interface signals:

Table 12: Video Memory Interface

Signal Name	I/O Type	Description
CAS#	O	Column Address Select

CKE	O	Clock Enable for Memory
CS#[1..0]	O	Chip Select for Memory
DQM[7..0]	O	Memory Data Byte Mask
DSF	O	Memory Special Function Enable
HCLK	O	Memory Clock
[11..0]	O	Memory Address Bus
MD[31..0]	I/O	Memory Data Bus
RAS#	O	Row Address Select
WE#	O	Write Enable

3.4.7.3 Dual video

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

- In single mode (Dual Monitor Video=**Disabled**), the onboard video controller is disabled when an add-in video card is detected.

- In dual mode (Onboard Video=**Enabled**, Dual Monitor Video=**Enabled**), the onboard video controller is enabled and will be the primary video device. The external video card will be allocated resources and is considered the secondary video device. BIOS Setup provides user options to configure the feature as follows:

-

Onboard Video	**Enabled** Disabled		
Dual Monitor Video	**Enabled** Disabled		Shaded if onboard video is set to "Disabled"

3.4.8 Network Interface Controller (NIC)

The Intel 82546GB dual-channel gigabit network interface controller supplies the baseboard with two network interfaces. The 82546GB is a highly integrated PCI LAN controller in a 21 mm^2 PBGA package. Each channel is capable of supporting 10/100/1000 operation and alert-on-LAN functionality. Both channels can be disabled by using the BIOS Setup utility, which is accessed during POST. The 82546GB supports the following features:

- 64-bit PCI-X Rev. 1.0 master interface
- Integrated IEEE 802.3 10Base-T, 100Base-TX and 1000Base-TX compatible PHY
- IEEE 820.3ab auto-negotiation support
- Full duplex support at 10 Mbps, 100Mbps and 1000 Mbps operation
- Integrated UNDI ROM support
- MDI/MDI-X and HWI support
- Low power +3.3 V device

3.4.8.1 NIC Connector and Status LEDs

The 82546GB drives the two LEDs that are located on each network interface connector. The link/activity LED to the left of the connector indicates network connection when on, and transmit/receive activity when blinking. The speed LED to the right of the connector indicates 1000Mbps operations when amber, 100Mbps operations when green, and 10-Mbps when off.

3.4.9 USB 2.0 Support

The USB controller functionality integrated into ICH5-R provides the baseboard with the interface for up to six USB 2.0 ports. Two external connectors are located on the back edge of the baseboard. Two 10 pin internal on-board headers are provided which are each capable of supporting an additional two optional connectors.

Legacy USB
The BIOS supports PS/2 emulation of USB 1.1 keyboards and mice. During POST, the BIOS initializes and configures the root hub ports and then searches for a keyboard and mouse. If detected, the USB hub enables them.

3.4.10 Super I/O Chip

Legacy I/O support is provided by using a National Semiconductor* PC87427 Super I/O device. This chip contains all of the necessary circuitry to control two serial ports, one parallel port, floppy disk, and PS/2-compatible keyboard and mouse. Of these, the Server Board SE7520JR2 supports the following:

- GPIOs
- Two serial ports
- Floppy Controller
- Keyboard and mouse controller
- Wake up control

3.4.10.1 GPIOs

The National Semiconductor* PC87427 Super I/O provides nine general-purpose input/output pins that the Server Board SE7520JR2 utilizes. The following table identifies the pin and the signal name used in the schematic:

Table 13: Super I/O GPIO Usage Table

Pin	Name	IO/GPIO	SE7520JR2 Use
124	GPIO00/CLKRUN_L	I/O	TP
125	GPIO01/KBCLK	I/O	KB_CLK
126	GPIO02/KBDAT	I/O	KB_DAT
127	GPIO03/MCLK	I/O	MS_CLK
128	GPIO04/MDAT	I/O	MS_DAT
9	GPIO05/XRDY	I/O	TP
10	GPIO06/XIRQ	I/O	BMC_SYSIRQ
13	GPIO07/HFCKOUT	I/O	SIO_CLK_40M_BMC
1	GPIOE10/XA11	I/O,I(E)1	XBUS_A<11>

Pin	Name	IO/GPIO	SE7520JR2 Use
2	GPIOE11/XA10	I/O,I(E)1	XBUS_A<10>
3	GPIOE12/XA9	I/O,I(E)1	XBUS_A<9>
4	GPIOE13/XA8	I/O,I(E)1	XBUS_A<8>
5	GPIOE14/XA7	I/O,I(E)1	XBUS_A<7>
6	GPIOE15/XA6	I/O,I(E)1	XBUS_A<6>
7	GPIOE16/XA5	I/O,I(E)1	XBUS_A<5>
8	GPIOE17/XA4	I/O,I(E)1	XBUS_A<4>
14	GPIO20/XRD_XEN_L	I/O	XBUS_XRD_L
15	GPIO21/XWR_XRW_L	I/O	XBUS_XWR_L
16	GPIO22/XA3	I/O	XBUS_A<3>
17	GPIO23/XA2	I/O	XBUS_A<2>
18	GPIO24/XA1	I/O	XBUS_A<1>
19	GPIO25/XA0	I/O	XBUS_A<0>
22	GPIO26/XCS1_L	I/O	TP
23	GPIO27/XCS0_L	I/O	XBUS_XCS0_L
24	GPIO30/XD7	I/O	XBUS_D<7>
25	GPIO31/XD6	I/O	XBUS_D<6>
26	GPIO32/XD5	I/O	XBUS_D<5>
27	GPIO33/XD4	I/O	XBUS_D<4>
28	GPIO34/XD3	I/O	XBUS_D<3>
29	GPIO35/XD2	I/O	XBUS_D<2>
30	GPIO36/XD1	I/O	XBUS_D<1>
31	GPIO37/XD0	I/O	XBUS_D<0>
20	GPIOE40/XCS3_L	I/O,I(E)1	TP
21	GPIOE41/XCS2_L	I/O,I(E)1	TP
35	GPIOE42/SLBTIN_L	I/O,I(E)1	TP
49	GPIOE43/PWBTOUT_L	I/O,I(E)1	ZZ_POST_CLK_LED_L
50	GPIOE44/LED1	I/O,I(E)1	ZZ_BIOS_ROLLING
51	GPIOE45/LED2	I/O,I(E)1	FP_PWR_LED_L
52	GPIOE46/SLPS3_L	I/O,I(E)1	TP
53	GPIOE47/SLPS5_L	I/O,I(E)1	TP
36	GPIO50/PWBTN_L	I/O	TP
37	GPIO51/SIOSMI_L	I/O	TP
38	GPIO52/SIOSCI_L	I/O	SIO_PME_L
45	GPIO53/LFCKOUT/MSEN0	I/O	TP
54	GPIO54/VDDFELL	I/O	ZZ_POST_DATA_LED_L
56	GPIO55/CLKIN	I/O	CLK_48M_SIO
32	GPO60/XSTB2/XCNF2_L	O	PU_XBUS_XCNF2
33	GPO61/XSTB1/XCNF1_L	O	XBUS_XSTB1_L
34	GPO62/XSTB0/XCNF0_L	O	PU_XBUS_XCNF0
48	GPO63/ACBSA	O	PU_SIO_ACBSA
55	GPO64/WDO_L/CKIN48	O	PU_SIO_CKIN48

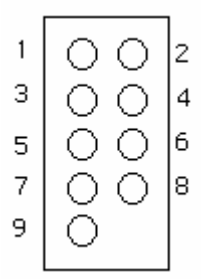
3.4.10.2 Serial Ports

The baseboard provides two serial ports: an external RJ45 Serial B port, and an internal DH10 Serial A header. The following sub-sections provide details on the use of the serial ports.

3.4.10.2.1 Serial Port A

Serial A is an optional port, accessed through a 9-pin internal DH-10 header. A standard DH10 to DB9 cable is used to direct Serial A out the back of a given chassis. The Serial A interface follows the standard RS232 pin-out as defined in the following table.

Table 14: Serial A Header Pin-out

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

3.4.10.2.2 Serial Port B

Serial B is an external 8-pin RJ45 connector that is located on the back edge of the baseboard. For serial devices that require a DB-9 connector, an appropriate RJ45-to-DB9 adapter is necessary.

3.4.10.2.3 Serial Port Multiplexer Logic

The Server Board SE7520JR2 has a multiplexer to connect the rear RJ45 connector to either Serial Port A or Serial Port B. This facilitates the routing of Serial Port A to the rear RJ45 connector if Serial Port B is used for Serial Over LAN (SOL). This serial port selection can be done through the BIOS setup option.

The figure below shows the serial port mux functionality.

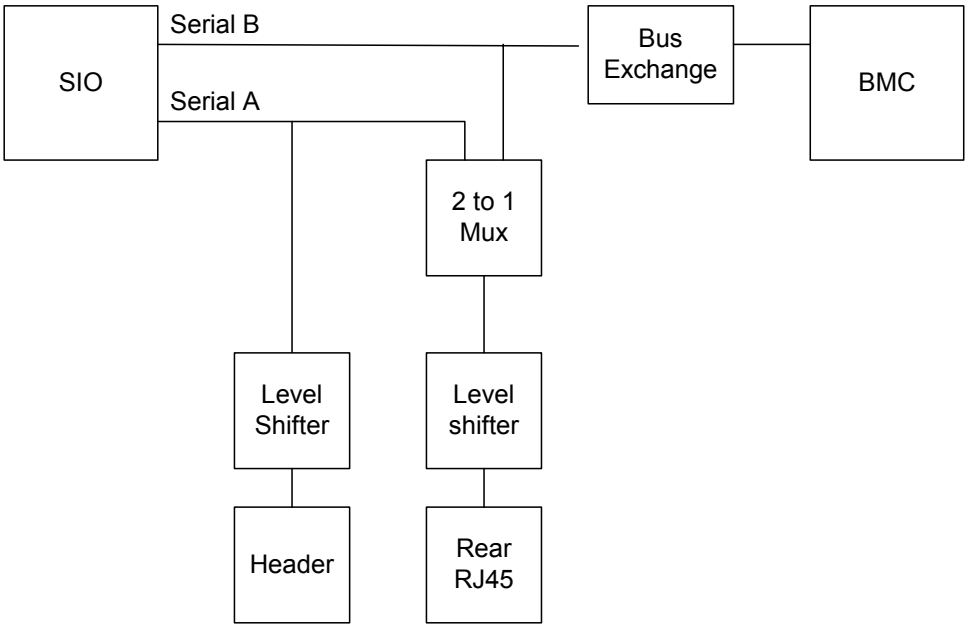


Figure 12. Serial Port Mux Logic

3.4.10.2.4 Rear RJ45 Serial B Port Configuration

The rear RJ45 Serial B port is a fully functional serial port that can support any standard serial device. Using an RJ45 connector for a serial port gives direct support for serial port concentrators, which are widely used in the high-density server market. For server applications that use a serial concentrator to access the server management features of the baseboard, a standard 8-pin CAT-5 cable from the serial concentrator is plugged directly into the rear RJ45 serial port.

To support either of two serial port configuration standards which require either a DCD or DSR signal, a jumper block (J7A1), located near the back IO ports, is used to configure the RJ45 serial port to the desired standard. The following diagram shows the jumper block location and its jumper settings.

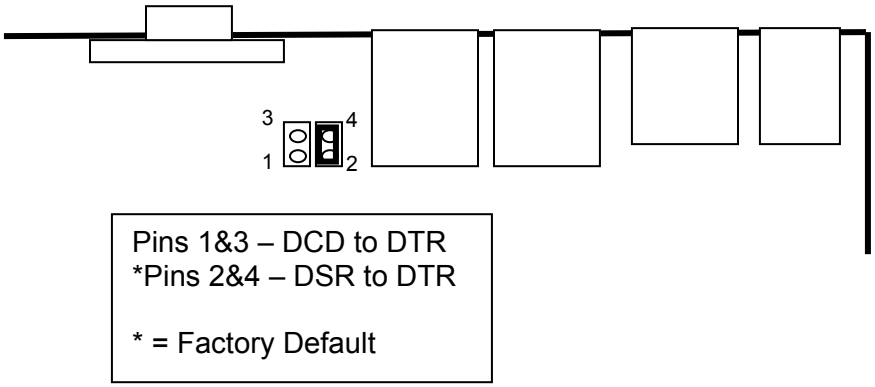


Figure 13. RJ45 Serial B Port Jumper Block Location and Setting

Note: The appropriate RJ45-to-DB9 adapter should match the configuration of the serial device used. One of two pin-out configurations is used, depending on whether the serial device requires a DSR or DCD signal. The final adapter configuration should also match the desired pin-out of the RJ45 connector, as it can also be configured to support either DSR or DCD.

3.4.10.3 Removable Media Drives

The BIOS supports removable media devices, including 1.44MB floppy removable media devices and optical devices such as a CD-ROM drive or DVD drive (read only). The BIOS supports booting from USB mass storage devices connected to the chassis USB port, such as a USB key device.

The BIOS supports USB 2.0 media storage devices that are backward compatible to the USB 1.1 specification.

3.4.10.4 Floppy Disk Support

The floppy disk controller (FDC) in the SIO is functionally compatible with floppy disk controllers in the DP8473 and N844077. All FDC functions are integrated into the SIO including analog data separator and 16-byte FIFO. On the Server Board SE7520JR2, floppy controller signals are directed to two separate connectors. When the baseboard is used with any of the backplanes designed for either the Server Chassis SR1400 or SR2400, the floppy signals are directed through the 100-pin backplane connector (J2J1). If no backplane is present, a floppy drive can be attached to the on-board legacy 36-pin connector (J3K2).

Note: Using both interfaces in a common configuration is not supported.

3.4.10.5 Keyboard and Mouse Support

Dual stacked PS/2 ports, located on the back edge of the baseboard, are provided for keyboard and mouse support. Either port can support a mouse or keyboard. Neither port will support “Hot Plugging” or connector insertion while the system is turned on.

The system can boot without a keyboard. If present, the BIOS detects the keyboard during POST and displays the message “Keyboard Detected” on the POST Screen

3.4.10.6 Wake-up Control

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

3.4.11 BIOS Flash

The BIOS supports the Intel® 28F320C3B flash part. The flash part is a 4-MB flash ROM with 2MB programmable. The flash ROM contains system initialization routines, setup utility, and runtime support routines. The exact layout is subject to change, as determined by Intel. A 128-KB block is available for storing OEM code (user binary) and custom logos.

3.5 Configuration and Initialization

This section describes the initial programming environment including address maps for memory and I/O, techniques and considerations for programming ASIC registers, and hardware options configuration.

3.5.1 Memory Space

At the highest level, the Intel Xeon processor address space is divided into four regions, as shown in the following figure. Each region contains the sub-regions that are described in following sections. Attributes can be independently assigned to regions and sub-regions using registers. The Intel E7520 chipset supports 64GB of host-addressable memory space and 64KB+3 of host-addressable I/O space. The Server Board SE7520JR2 supports only the main memory up to 24GB for DDR-266 or up to 16GB for DDR333/DDR2-400.

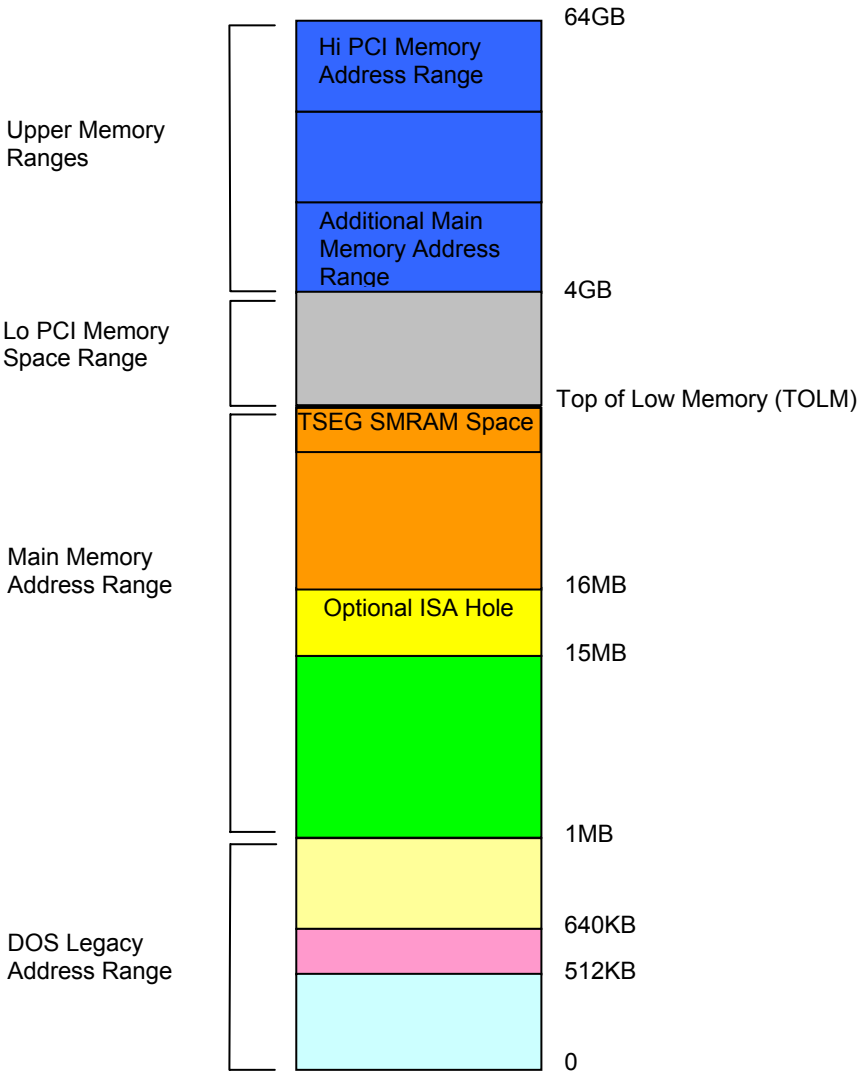


Figure 14. Intel® Xeon™ Processor Memory Address Space

3.5.1.1 DOS Compatibility Region

The first region of memory below 1 MB was defined for early PCs, and must be maintained for compatibility reasons. The region is divided into sub-regions as shown in the following figure.

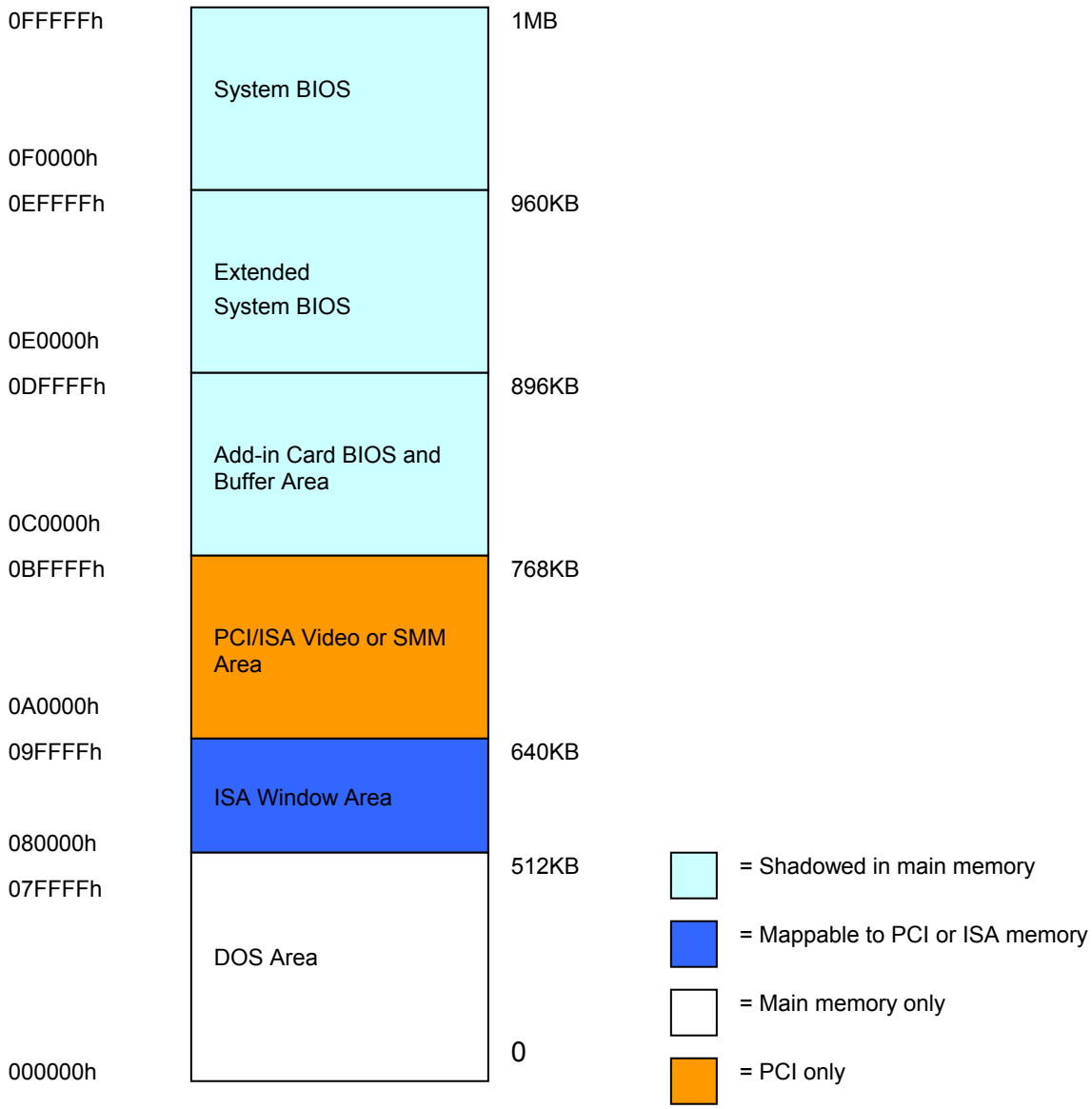


Figure 15. DOS Compatibility Region

3.5.1.1.1 DOS Area

The DOS region is 512 KB in the address range 0 to 07FFFFh. This region is fixed and all accesses go to main memory.

3.5.1.1.2 ISA Window Memory

The ISA Window Memory is 128 KB between the address of 080000h to 09FFFFh. This area can be mapped to the PCI bus or main memory.

3.5.1.1.3 Video or SMM Memory

The 128 KB Graphics Adapter Memory region at 0A0000h to 0BFFFFh is normally mapped to the VGA controller on the PCI bus. This region is also the default region for SMM space.

3.5.1.1.4 Add-in Card BIOS and Buffer Area

The 128 KB region between addresses 0C0000h to 0DFFFFh is divided into eight segments of 16 KB segments mapped to ISA memory space, each with programmable attributes, for expansion cards buffers. Historically, the 32 KB region from 0C0000h to 0C7FFFh has contained the video BIOS location on the video card

3.5.1.1.5 Extended System BIOS

This 64 KB region from 0E0000h to 0EFFFFh is divided into four blocks of 16 KB each, and may be mapped with programmable attributes to map to either main memory or to the PCI bus. Typically this area is used for RAM or ROM. This region can also be used extended SMM space.

3.5.1.1.6 System BIOS

The 64 KB region from 0F0000h to 0FFFFFh is treated as a single block. By default, this area is normally read/write disabled with accesses forwarded to the PCI bus. Through manipulation of read/write attributes, this region can be shadowed into main memory.

3.5.1.2 Extended Memory

Extended memory is defined as all address space greater than 1MB. Extended Memory region covers 8GB maximum of address space from addresses 0100000h to FFFFFFFh, as shown in the following figure. PCI memory space can be remapped to top of memory (TOM).

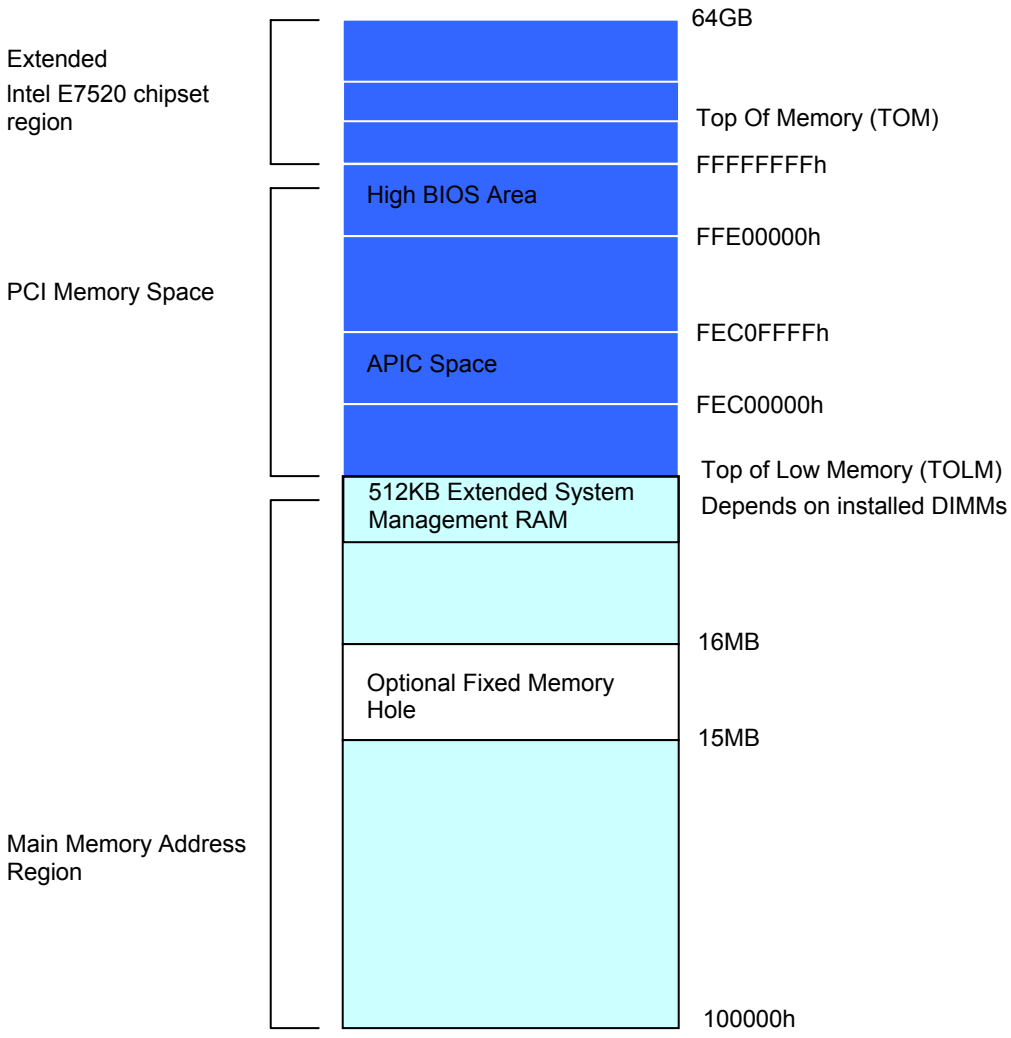


Figure 16. Extended Memory Map

3.5.1.2.1 Main Memory

All installed memory greater than 1MB is mapped to local main memory, up to 8GB of physical memory. Memory between 1MB to 15MB is considered to be standard ISA extended memory. 1MB of memory starting at 15MB can be optionally mapped to the PCI bus memory space.

The remainder of this space, up to 8GB, is always mapped to main memory, unless TBSG SMM is used which is just under TOLM. The range can be from 128KB till 1MB. 1MB depends on the BIOS setting C SMRAM is used which limits the top of memory to 256MB. The BIOS occupies 512KB for the 32-bit SMI handler.

3.5.1.2.2 PCI Memory Space

Memory addresses below the 4GB range are mapped to the PCI bus. This region is divided into three sections: High BIOS, APIC configuration space, and general-purpose PCI memory. The General-purpose PCI memory area is typically used memory-mapped I/O to PCI devices. The memory address space for each device is set using PCI configuration registers.

3.5.1.2.3 High BIOS

The top 1MB of extended memory under 4GB is reserved for the system BIOS, extended BIOS for PCI devices, and A20 aliasing by the system BIOS. The Intel Xeon processor begins executing from the high BIOS region after reset.

3.5.1.2.4 High Memory Gap Reclaiming

The BIOS creates a region immediately below 4 GB to accommodate memory-mapped I/O regions for the system BIOS Flash, APIC memory and 32-bit PCI devices. Any system memory in this region is remapped above 4GB.

3.5.1.2.5 I/O APIC Configuration Space

A 64KB block located 20MB below 4GB (0FEC00000 to 0FEC0FFFFh) is reserved for the I/O APIC configuration space. The first I/O APIC is located at FEC00000h. The second I/O APIC is located at FEC80000h. The third I/O APIC is located at FEC80100h.

3.5.1.2.6 Extended Intel® Xeon™ Processor Region (above 4GB)

An Intel Xeon processor based system can have up to 64 GB of addressable memory. With the chipset only supporting 16GB of addressable memory, the BIOS uses an extended addressing mechanism to use the address ranges.

3.5.1.3 Memory Shadowing

System BIOS and option ROM can be shadowed in main memory. Typically this is done to allow ROM code to execute more rapidly out of RAM. ROM is designated read-only during the copy process while RAM at the same address is designated write-only. After copying, the RAM is designated read-only. After the BIOS is shadowed, the attributes for that memory area are set to read only so that all writes are forwarded to the expansion bus.

3.5.1.4 System Management Mode Handling

The chipset supports System Management Mode (SMM) operation in one of three modes. System Management RAM (SMRAM) provides code and data storage space for the SMI_L handler code, and is made visible to the processor only on entry to SMM, or other conditions that can be configured using Intel Lindenhurst PF chipset.

The MCH supports three SMM options:

- Compatible SMRAM (C_SMRAM)
- High Segment (HSEG)
- Top of Memory Segment (TSEG)

Three abbreviations are used later in the table that describes SMM Space Transaction Handling.

SMM Space Enabled	Transaction Address Space (Adr)	DRAM Space (DRAM)
Compatible (C)	A0000h to BFFFFh	A0000h to BFFFFh
High (H)	0FEDA0000h TO 0FEDBFFFFh	A0000h to BFFFFh
TSEG (T)	(TOLM-TSEG_SZ) to TOLM	(TOLM-TSEG_SZ) to TOLM

Note: High SMM is different than in previous chipsets. In previous chipsets the high segment was the 384KB region from A_0000h to F_FFFFh. However C_0000h to F_FFFFh was not useful so it is deleted in MCH.

Note: TSEG SMM is different than in previous chipsets. In previous chipsets, the TSEG address space was offset by 256MB to allow for simpler decoding and the TSEG was remapped to directly under the TOLM. In the MCH, the TSEG region is not offset by 256MB and it is not remapped.

Table 15: SMM Space Table

Global Enable G_SMRAME	High Enable H_SMRAME	TSEG Enable TSEG_EN	Compatible (C) Range	High (H) Range	TSEG (T) Range
0	X	X	Disable	Disable	Disable
1	0	0	Enable	Disable	Disable
1	0	1	Enable	Disable	Enable
1	1	0	Disable	Enable	Disable
1	1	1	Disable	Enable	Enable

3.5.2 I/O Map

The baseboard I/O addresses are mapped to the processor bus or through designated bridges in a multi-bridge system. Other PCI devices, including the ICH5-R, have built-in features that support PC-compatible I/O devices and functions, which are mapped to specific addresses in I/O space. On SE7520JR2, the ICH5-R provides the bridge to ISA functions.

The I/O map in the following table shows the location in I/O space of all direct I/O-accessible registers. PCI configuration space registers for each device control mapping in I/O and memory spaces, and other features that may affect the global I/O map.

Table 16: I/O Map

Address (es)	Resource	Notes
0000h – 000Fh	DMA Controller 1	
0010h – 001Fh	DMA Controller 2	Aliased from 0000h – 000Fh
0020h – 0021h	Interrupt Controller 1	
0022h – 0023h		
0024h – 0025h	Interrupt Controller 1	Aliased from 0020 – 0021h
0026h – 0027h		
0028h – 0029h	Interrupt Controller 1	Aliased from 0020h – 0021h
002Ah – 002Bh		
002Ch – 002Dh	Interrupt Controller 1	Aliased from 0020h – 0021h
002Eh – 002Fh	Super I/O (SIO) index and Data ports	
0030h – 0031h	Interrupt Controller 1	Aliased from 0020h – 0021h
0032h – 0033h		
0034h – 0035h	Interrupt Controller 1	Aliased from 0020h – 0021h
0036h – 0037h		
0038h – 0039h	Interrupt Controller 1	Aliased from 0020h – 0021h
003Ah – 003Bh		
003Ch – 003Dh	Interrupt Controller 1	Aliased from 0020h – 0021h
003Eh – 003Fh		
0040h – 0043h	Programmable Timers	
0044h – 004Fh		
0050h – 0053F	Programmable Timers	
0054h – 005Fh		
0060h, 0064h	Keyboard Controller	Keyboard chip select from 87417
0061h	NMI Status & Control Register	
0063h	NMI Status & Control Register	Aliased
0065h	NMI Status & Control Register	Aliased
0067h	NMI Status & Control Register	Aliased
0070h	NMI Mask (bit 7) & RTC address (bits 6::0)	
0072h	NMI Mask (bit 7) & RTC address (bits 6::0)	Aliased from 0070h
0074h	NMI Mask (bit 7) & RTC address (bits 6::0)	Aliased from 0070h
0076h	NMI Mask (bit 7) & RTC address (bits 6::0)	Aliased from 0070h

Address (es)	Resource	Notes
0071h	RTC Data	
0073h	RTC Data	Aliased from 0071h
0075h	RTC Data	Aliased from 0071h
0077h	RTC Data	Aliased from 0071h
0080h – 0081h	BIOS Timer	
0080h – 008F	DMA Low Page Register	
0090h – 0091h	DMA Low Page Register (aliased)	
0092h	System Control Port A (PC-AT control Port) (this port not aliased in DMA range)	
0093h – 009Fh	DMA Low Page Register (aliased)	
0094h	Video Display Controller	
00A0h – 00A1h	Interrupt Controller 2	
00A4h – 00A5h	Interrupt Controller 2 (aliased)	
00A8h – 00A9h	Interrupt Controller 2 (aliased)	
00ACh – 00ADh	Interrupt Controller 2 (aliased)	
00B0h – 00B1h	Interrupt Controller 2 (aliased)	
00B4h – 00B5h	Interrupt Controller 2 (aliased)	
00B8h – 00B9h	Interrupt Controller 2 (aliased)	
00BCh – 00BDh	Interrupt Controller 2 (aliased)	
00C0h – 00DFh	DMA Controller 2	
00F0h	Clear NPX error	Resets IRQ13
00F8h – 00FFh	X87 Numeric Coprocessor	
0102h	Video Display Controller	
0170h – 0177h	Secondary Fixed Disk Controller (IDE)	
01F0h – 01F7h	Primary Fixed Disk Controller (IDE)	
0200h – 0207h	Game I/O Port	
0220h – 022Fh	Serial Port A	
0238h – 023Fh	Serial Port B	
0278h – 027Fh	Parallel Port 3	
0290h – 0298h	NS HW monitor	
02E8h – 02EFh	Serial Port B	
02F8h – 02FFh	Serial Port B	
0338h – 033Fh	Serial Port B	
0370h – 0375h	Secondary Floppy	
0376h	Secondary IDE	
0377h	Secondary IDE/Floppy	
0378h – 037Fh	Parallel Port 2	
03B4h – 03Bah	Monochrome Display Port	
03BCh – 03BFh	Parallel Port 1 (Primary)	
03C0h – 03CFh	Video Display Controller	
03D4h – 03Dah	Color Graphics Controller	
03E8h – 03Efh	Serial Port A	
03F0h – 03F5h	Floppy Disk Controller	
03F6h – 03F7h	Primary IDE – Sec Floppy	

Address (es)	Resource	Notes
03F8h – 03FFh	Serial Port A (primary)	
0400h – 043Fh	DMA Controller 1, Extended Mode Registers	
0461h	Extended NMI / Reset Control	
0480h – 048Fh	DMA High Page Register	
04C0h – 04CFh	DMA Controller 2, High Base Register	
04D0h – 04D1h	Interrupt Controllers 1 and 2 Control Register	
04D4h – 04D7h	DMA Controller 2, Extended Mode Register	
04D8h – 04DFh	Reserved	
04E0h – 04FFh	DMA Channel Stop Registers	
051Ch	Software NMI (051Ch)	
0678h – 067Ah	Parallel Port (ECP)	
0778h – 077Ah	Parallel Port (ECP)	
07BCh – 07Beh	Parallel Port (ECP)	
0CF8h	PCI CONFIG_ADDRESS Register	
0CF9h	Intel® Server Board SE7520JR2 Turbo and Reset Control	
0CFCh	PCI CONFIG_DATA Register	

3.5.3 Accessing Configuration Space

All PCI devices contain PCI configuration space, accessed using mechanism #1 defined in the PCI Local Bus Specification. If dual processors are used, only the processor designated as the Boot Strap Processor (BSP) should perform PCI configuration space accesses. Precautions must be taken to guarantee that only one processor performs system configuration.

Two Dword I/O registers in the chipset are used for the configuration space register access:

- CONFIG_ADDRESS (I/O address 0CF8h)
- CONFIG_DATA (I/O address 0CFCh)

When CONFIG_ADDRESS is written to with a 32-bit value selecting the bus number, device on the bus, and specific configuration register in the device, a subsequent read or write of CONFIG_DATA initiates the data transfer to/from the selected configuration register. Byte enables are valid during accesses to CONFIG_DATA; they determine whether the configuration register is being accessed or not. Only full Dword reads and writes to CONFIG_ADDRESS are recognized as a configuration access by the chipset. All other I/O accesses to CONFIG_ADDRESS are treated as normal I/O transactions.

3.5.3.1 CONFIG_ADDRESS Register

CONFIG_ADDRESS is 32 bits wide and contains the field format shown in the following figure. Bits [23::16] choose a specific bus in the system. Bits [15::11] choose a specific device on the selected bus. Bits [10:8] choose a specific function in a multi-function device. Bit [7::1] select a specific register in the configuration space of the selected device or function on the bus.

3.6 Clock Generation and Distribution

All buses on the baseboard operate using synchronous clocks. Clock synthesizer/driver circuitry on the baseboard generates clock frequencies and voltage levels as required, including the following:

- 200MHz differential clock at 0.7V logic levels. For Processor 0, Processor 1, Debug Port and MCH.
- 100MHz differential clock at 0.7V logic levels on CK409B. For DB800 clock buffer.
- 100MHz differential clock at 0.7 Vlogic levels on DB800. For PCI Express Device it is the MCH, PXH and full-length riser, which includes x4 PCI Express Slot. For SATA it is the ICH5-R.
- 66MHz at 3.3V logic levels: For MCH and ICH5-R.
- 48MHz at 3.3V logic levels: For ICH5-R and SIO.
- 33MHz at 3.3V logic levels: For ICH5-R, Video, BMC and SIO.
- 14.318MHz at 2.5V logic levels: For ICH5-R and video.
- 10Mhz at 5V logic levels: For mBMC.

The PCI-X slot speed on the full-length riser card and on the low-profile riser card is determined by the riser card in use.

4. System BIOS

The BIOS is implemented as firmware that resides in the Flash ROM. It provides hardware-specific initialization algorithms and standard PC-compatible basic input/output (I/O) services, and standard Intel® Server Board features. The Flash ROM also contains firmware for certain embedded devices. These images are supplied by the device manufacturers and are not specified in this document.

The system BIOS includes the following components:

- IA-32 Core – The IA-32 core contains standard services and components such as the PCI Resource manager, ACPI support, POST, and runtime functionality.
- Manageability Extensions – Intel servers build server management into the BIOS through the Intelligent Platform Management Interface (IPMI) and baseboard management hardware.
- Extensible Firmware Interface – "EFI" provides an abstraction layer between the operating system and system hardware.
- Processor Microcode – BIOS includes microcode for the latest processors.
- Option ROMs – BIOS includes option ROMs to enable on-board devices during boot.

4.1 BIOS Identification String

The BIOS Identification string is used to uniquely identify the revision of the BIOS being used on the system. The string is formatted as illustrated in the following figure.

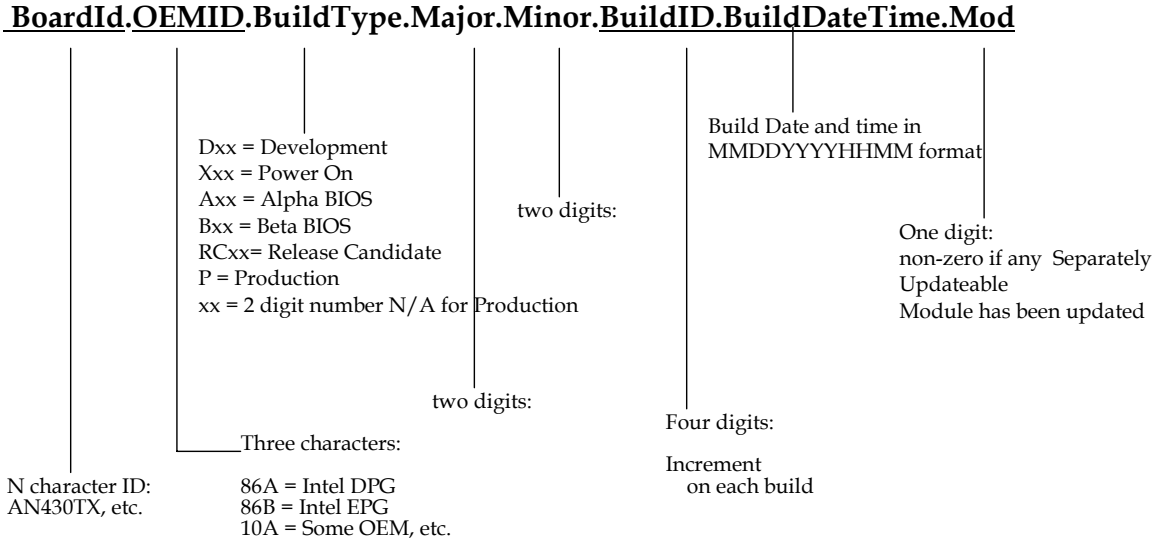


Figure 17. BIOS Identification String

As such, the BIOS ID for this platform takes the following form:

- SE7520JR2 supporting DDR memory
  SE7520JR22.86B.P.01.00.0002.081320031156

- SE7520JR2 supporting DDR2 memory
  SE7520JR23.86B.P.01.00.0002.081320031156

4.2 Flash Architecture and Flash Update Utility

The flash ROM contains system initialization routines, the BIOS Setup Utility, and runtime support routines. The exact layout is subject to change, as determined by Intel. A 64-KB user block is available for user ROM code or custom logos. The flash ROM also contains initialization code in compressed form for onboard peripherals, like SCSI, NIC and video controllers. It also contains support for the rolling single-boot BIOS update feature.

4.3 BIOS Power On Self Test (POST)

The BIOS Power On Self Test (POST) begins when the system is powered on. During POST, the BIOS initializes and tests various sub-systems, sets up all major system operating parameters, and gives the opportunity for any optionally installed add-in cards to execute setup code. When complete, and if no errors are encountered, BIOS turns control of the system over to the installed operating system.

As video is initialized during POST, the opportunity to view and alter the POST process is made available through either a locally attached monitor or through remote console redirection.

4.3.1 User Interface

During the system boot-up POST process, there are two types of consoles used for displaying the user interface: graphical or text based. Graphics consoles are in 640x480 mode; text consoles use 80x25 mode.

The console output is partitioned into three windows: the System Activity/State, Splash Screen/Diagnostic, and POST Activity. The POST Activity window displays information about the current state of the system. The Splash Screen / Diagnostic window displays the OEM splash screen or a diagnostic information screen. The POST Activity window displays information about the currently executing portion of POST as well as user prompts and status messages.

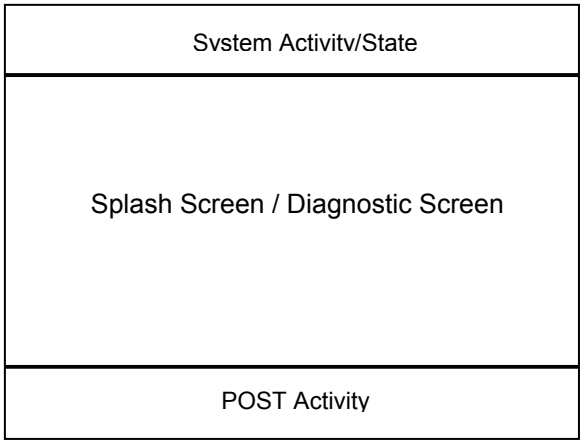


Figure 18. POST Console Interface

4.3.1.1 System Activity Window

The top row of the screen is reserved for the system state window. On a graphics console, the window is 640x48. On a text console, the window is 80x2.

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.

4.3.1.2 Splash Screen/Diagnostic Window

The middle portion of the screen is reserved for either a splash screen or diagnostic screen. On a graphics console, the window is 640x384. On a text console, the window is 80x20.

In the BIOS Setup Utility, The Quiet Boot option is used to select which of the two screens is displayed. If Quiet Boot is set to Enabled, a splash screen programmed into the BIOS is displayed, hiding any POST progress information. If the Quiet Boot option is Disabled, all POST progress information will be displayed to the screen. The factory default is to have the Quiet Boot option enabled, displaying the Splash Screen. However, if during the POST process the <ESC> key is pressed while the Splash Screen is being displayed, the view will change to the diagnostic screen for the current boot only

4.3.1.2.1 System Diagnostic Screen

The diagnostic screen is the console where boot information, options and detected hardware information are displayed.

The Static Information Display area presents the following information:

- Copyright message
- BIOS ID
- Current processor configuration
- Installed physical memory size

4.3.1.2.2 Quiet Boot / OEM Splash Screen

The BIOS implements Quiet Boot, providing minimal startup display during BIOS POST. System start-up must only draw the end user's attention in the event of errors or when there is a need for user action. By default, the system must be configured so that the local screen does not display memory counts, device status, etc. It must present a "clean" BIOS start-up. The only screen display allowed is the OEM splash screen and copyright notices.

The Quiet Boot process is controlled by a Setup Quiet-Boot option. If this option is set, the BIOS displays an activity indicator at the top of the screen and a logo splash screen in the middle section of the screen on the local console. The activity indicator measures POST progress and continues until the operating system gains control of the system. The splash screen covers up any diagnostic messages in the middle section of the screen. While the logo is being displayed on the local console, diagnostic messages are being displayed on the remote text consoles.

Quiet Boot may be disabled by disabling the Setup Quiet-Boot option or by the user pressing the <Esc> key while in Quiet Boot mode. If Quiet Boot is disabled, the BIOS displays diagnostic messages in place of the activity indicator and the splash screen.

With the use of an Intel supplied utility, the BIOS allows OEMs to override the standard Intel logo with one of their own design

4.3.1.3 POST Activity Window

The bottom portion of the screen is reserved for the POST Activity window. On a graphics console, the window is 640x48. On a text console, the window is 80x2.

The POST Activity window is used to display prompts for hot keys, as well as provide information on system status.

4.3.2 BIOS Boot Popup Menu

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

Table 17: Sample BIOS Popup Menu

Please select boot device:
1st Floppy Hard Drives ATAPI CDROM LAN PXE EFI Boot Manager
↓and↑ to move selection Enter to select boot device ESC to boot using defaults

4.4 BIOS Setup Utility

The BIOS Setup utility is provided to perform system configuration changes and to display current settings and environment information.

The BIOS Setup utility stores configuration settings in system non-volatile storage. Changes affected by BIOS Setup will not take effect until the system is rebooted. The BIOS Setup Utility can be accessed during POST by using the <F2> key.

4.4.1 Localization

The BIOS Setup utility uses the Unicode standard and is capable of displaying Setup screens in English, French, Italian, German, and Spanish. The BIOS supports these languages for console strings as well.

Keyboard Commands
While in the BIOS Setup utility, the Keyboard Command Bar supports the keys specified in the following table.

Table 18: BIOS Setup Keyboard Command Bar Options

Key	Option	Description
Enter	Execute Command	The Enter key is used to activate sub-menus, pick lists, or to select a sub-field. If a pick list is displayed, the Enter key will select the pick list highlighted item, and pass that selection in 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 continues with POST.
↑	Select Item	The up arrow is used to select the previous value in a pick list, or the previous options 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.

Key	Option	Description
↔	Select Menu	The left and right arrow keys are used to move between the major menu pages. The keys have no affect if a sub-menu or pick list is displayed.
Tab	Select Field	The Tab key is used to move between fields. For example, Tab can be used to move from hours to minutes in the time item in the main menu.
-	Change Value	The minus key on the keypad is used to change the value of the current item to the previous value. This key scrolls through the values in the associated pick list without displaying the full list.
+	Change Value	The plus key on the keypad is used to change the value of the current menu item to the next value. This key scrolls through the values in the associated pick list without displaying the full list. On 106-key Japanese keyboards, the plus key has a different scan code than the plus key on the other keyboard, but will have the same effect.
F9	Setup Defaults	Pressing F9 causes the following to appear: **Load Setup Defaults?** **[OK] [Cancel]** If “OK” is selected and the Enter key is pressed, all setup fields are set to their default values. If “Cancel” is selected and the Enter 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.
F7	Discard Changes	Pressing F7 causes the following message to appear: **Discard Changes?** **[OK] [Cancel]** If “OK” is selected and the Enter key is pressed, all changes are not saved and setup is exited. If “Cancel” is selected and the Enter key is pressed, or the ESC key is pressed, the user is returned to where they were before F7 was pressed without affecting any existing values.
F10	Save Changes and Exit	Pressing F10 causes the following message to appear: **Save configuration changes and exit setup?** **[OK] [Cancel]** If “OK” is selected and the Enter key is pressed, all changes are saved and setup is exited. If “Cancel” is selected and the Enter 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.

4.4.2 Entering BIOS Setup

The BIOS Setup utility is accessed by pressing the <F2> hotkey during POST

4.4.2.1 Main Menu

The first screen displayed when entering the BIOS Setup Utility is the Main Menu selection screen. This screen displays the major menu selections available. The following tables describe the available options on the top level and lower level menus. Default values are shown in **bold** text.

Table 19: BIOS Setup, Main Menu Options

Feature	Options	Help Text	Description

Feature	Options	Help Text	Description
System Overview			
AMI BIOS			
Version	N/A	N/A	BIOS ID string (excluding the build time and date)
Build Date	N/A	N/A	BIOS build date
Processor			
Type	N/A	N/A	Processor brand ID string
Speed	N/A	N/A	Calculated processor speed
Count	N/A	N/A	Detected number of physical processors
System Memory			
Size	N/A	N/A	Amount of physical memory detected
System Time	HH:MM:SS	Use [ENTER], [TAB] or [SHIFT-TAB] to select a field. Use [+] or [-] to configure system Time.	Configures the system time on a 24 hour clock. Default is 00:00:00
System Date	DAY MM/DD/YYYY	Use [ENTER], [TAB] or [SHIFT-TAB] to select a field. Use [+] or [-] to configure system Date.	Configures the system date. Default is [Build Date]. Day of the week is automatically calculated.
Language	**English** French German Italian Spanish	Select the current default language used by the BIOS.	Select the current default language used by BIOS.

4.4.2.2 Advanced Menu

Table 20: BIOS Setup, Advanced Menu Options

Feature	Options	Help Text	Description
Advanced Settings			
WARNING: Setting wrong values in below sections may cause system to malfunction.			
Processor Configuration	N/A	Configure processors.	Selects submenu.
IDE Configuration	N/A	Configure the IDE device(s).	Selects submenu.
Floppy Configuration	N/A	Configure the Floppy drive(s).	Selects submenu.
Super I/O Configuration	N/A	Configure the Super I/O Chipset.	Selects submenu.
USB Configuration	N/A	Configure the USB support.	Selects submenu.
PCI Configuration	N/A	Configure PCI devices.	Selects submenu.
Memory Configuration	N/A	Configure memory devices.	Selects submenu.

4.4.2.2.1 Processor Configuration Sub-menu

Table 21: BIOS Setup, Processor Configuration Sub-menu Options

Feature	Options	Help Text	Description
Configure Advanced Processor Settings			
Manufacturer	Intel	N/A	Displays processor manufacturer string
Brand String	N/A	N/A	Displays processor brand ID string
Frequency	N/A	N/A	Displays the calculated processor speed
FSB Speed	N/A	N/A	Displays the processor front-side bus speed.
CPU 1			
CPUID	N/A	N/A	Displays the CPUID of the processor.
Cache L1	N/A	N/A	Displays cache L1 size.
Cache L2	N/A	N/A	Displays cache L2 size.
Cache L3	N/A	N/A	Displays cache L3 size. Visible only if the processor contains an L3 cache.
CPU 2			
CPUID	N/A	N/A	Displays the CPUID of the processor.
Cache L1	N/A	N/A	Displays cache L1 size.
Cache L2	N/A	N/A	Displays cache L2 size.
Cache L3	N/A	N/A	Displays cache L3 size. Visible only if the processor contains an L3 cache.
Processor Retest	**Disabled** Enabled	If enabled, all processors will be activated and retested on the next boot. This option will be automatically reset to disabled on the next boot.	Rearms the processor sensors. Only displayed if the Intel Management Module is present.
Max CPUID Value Limit	**Disabled** Enabled	This should be enabled in order to boot legacy OSes that cannot support processors with extended CPUID functions.	
Hyper-Threading Technology	Disabled **Enabled**	Enable Hyper-Threading Technology only if OS supports it.	Controls Hyper-Threading state. Primarily used to support older Operating Systems that do not support Hyper Threading.
Intel ® Speed Step ™ Tech	Auto **Disabled**	Select disabled for maximum CPU speed. Select enabled to allow the OS to reduce power consumption.	Note: This option may not be present in early Beta releases.

4.4.2.2.2 IDE Configuration Sub-menu

Table 22: BIOS Setup IDE Configuration Menu Options

Feature	Options	Help Text	Description
IDE Configuration			
Onboard P-ATA Channels	Disabled Primary Secondary **Both**	Disabled: disables the integrated P-ATA Controller. Primary: enables only the Primary P-ATA Controller. Secondary: enables only the Secondary P-ATA Controller. Both: enables both P-ATA Controllers.	Controls state of integrated P-ATA controller.
Onboard S-ATA Channels	Disabled **Enabled**	Disabled: disables the integrated S-ATA Controller. Enabled: enables the integrated S-ATA Controller.	Controls state of integrated S-ATA controller.
Configure S-ATA as RAID	**Disabled** Enabled	When enabled the S-ATA channels are reserved to be used as RAID.	
S-ATA Ports Definition	**A1-3rd M/A2-4th M** A1-4th M/A2-3rd M	Defines priority between S-ATA channels.	Default set the S-ATA Port0 to 3rd IDE Master channel & Port1 to 4th IDE Master channel. Otherwise set S-ATA Port0 to 4th IDE Master channel & Port1 to 3rd IDE Master channel.
Mixed P-ATA / S-ATA	N/A	Lets you remove a P-ATA and replace it by S-ATA in a given channel. Only 1 channel can be S-ATA.	Selects submenu for configuring mixed P-ATA and S-ATA.
Primary IDE Master	N/A	While entering setup, BIOS auto detects the presence of IDE devices. This displays the status of auto detection of IDE devices.	Selects submenu with additional device details.
Primary IDE Slave	N/A	While entering setup, BIOS auto detects the presence of IDE devices. This displays the status of auto detection of IDE devices.	Selects submenu with additional device details.
Secondary IDE Master	N/A	While entering setup, BIOS auto detects the presence of IDE devices. This displays the status of auto detection of IDE devices.	Selects submenu with additional device details.
Secondary IDE Slave	N/A	While entering setup, BIOS auto detects the presence of IDE devices. This displays the status of auto detection of IDE devices.	Selects submenu with additional device details.

Feature	Options	Help Text	Description
Third IDE Master	N/A	While entering setup, BIOS auto detects the presence of IDE devices. This displays the status of auto detection of IDE devices.	Selects submenu with additional device details.
Fourth IDE Master	N/A	While entering setup, BIOS auto detects the presence of IDE devices. This displays the status of auto detection of IDE devices.	Selects submenu with additional device details.
Hard Disk Write Protect	**Disabled** Enabled	Disable/Enable device write protection. This will be effective only if device is accessed through BIOS.	Primarily used to prevent unauthorized writes to hard drives.
IDE Detect Time Out (Sec)	0 5 10 15 20 25 30 **35**	Select the time out value for detecting ATA/ATAPI device(s).	Primarily used with older IDE devices with longer spin up times.
ATA(PI) 80Pin Cable Detection	**Host & Device** Host Device	Select the mechanism for detecting 80Pin ATA(PI) Cable.	The 80 pin cable is required for UDMA-66 and above. BIOS detects the cable by querying the host and/or device.

Table 23: Mixed P-ATA-S-ATA Configuration with only Primary P-ATA

Feature	Options	Help Text	Description
Mixed P-ATA / S-ATA			
First ATA Channel	**P-ATA M-S** S-ATA M-S	Configure this channel to P-ATA or S-ATA. P-ATA: Parallel ATA Primary channel. S-ATA: Serial ATA.	Defines the S-ATA device for this channel. If the Second ATA is assigned S-ATA, this option reverts to P-ATA.
Second ATA Channel	**P-ATA M-S** S-ATA M-S	Configure this channel to P-ATA or S-ATA. P-ATA: Parallel ATA Primary channel. S-ATA: Serial ATA.	Defines the S-ATA device for this channel. If the First ATA is assigned S-ATA, this option reverts to P-ATA.
3rd & 4th ATA Channels	**A1-3rd M/A2-4th M** A1-4th M/A2-3rd M None	Configure this channel to P-ATA or S-ATA. P-ATA: Parallel ATA Primary channel. S-ATA: Serial ATA.	Display only. If the First ATA or Second ATA is assigned S-ATA, this option reverts to None.

Table 24: BIOS Setup, IDE Device Configuration Sub-menu Selections

Feature	Options	Help Text	Description
Primary/Secondary/Third/Fourth IDE Master/Slave			
Device	N/A	N/A	Display detected device info
Vendor	N/A	N/A.	Display IDE device vendor.
Size	N/A	N/A	Display IDE DISK size.
LBA Mode	N/A	N/A	Display LBA Mode
Block Mode	N/A	N/A	Display Block Mode
PIO Mode	N/A	N/A	Display PIO Mode
Async DMA	N/A	N/A	Display Async DMA mode
Ultra DMA	N/A	N/A	Display Ultra DMA mode.
S.M.A.R.T.	N/A	N/A	Display S.M.A.R.T. support.
Type	Not Installed **Auto** CDROM ARMD	Select the type of device connected to the system.	The Auto setting should work in most cases.
LBA/Large Mode	Disabled **Auto**	Disabled: Disables LBA Mode. Auto: Enabled LBA Mode if the device supports it and the device is not already formatted with LBA Mode disabled.	The Auto setting should work in most cases.
Block (Multi-Sector Transfer) Mode	Disabled **Auto**	Disabled: The Data transfer from and to the device occurs one sector at a time. Auto: The data transfer from and to the device occurs multiple sectors at a time if the device supports it.	The Auto setting should work in most cases.
PIO Mode	**Auto** 0 1 2 3 4	Select PIO Mode.	The Auto setting should work in most cases.
DMA Mode	**Auto** SWDMA0-0 SWDMA0-1 SWDMA0-2 MWDMA0-0 MWDMA0-1 MWDMA0-2 UWDMA0-0 UWDMA0-1 UWDMA0-2 UWDMA0-3 UWDMA0-4 UWDMA0-5	Select DMA Mode. Auto :Auto detected SWDMA :SinglewordDMAn MWDMA :MultiwordDMAn UWDMA :UltraDMAn	The Auto setting should work in most cases.
S.M.A.R.T.	**Auto** Disabled Enabled	Self-Monitoring, Analysis and Reporting Technology.	The Auto setting should work in most cases.
32Bit Data Transfer	**Disabled** Enabled	Enable/Disable 32-bit Data Transfer	

4.4.2.2.3 Floppy Configuration Sub-menu

Table 25: BIOS Setup, Floppy Configuration Sub-menu Selections

Feature	Options	Help Text	Description
Floppy Configuration			
Floppy A	Disabled 720 KB 3 1/2" **1.44 MB 3 1/2"** 2.88 MB 3 1/2"	Select the type of floppy drive connected to the system.	Note: Intel no longer validates 720Kb & 2.88Mb drives.
Onboard Floppy Controller	Disabled **Enabled**	Allows BIOS to Enable or Disable Floppy Controller.	

4.4.2.2.4 Super I/O Configuration Sub-menu

Table 26: BIOS Setup, Super I/O Configuration Sub-menu

Feature	Options	Help Text	Description
Configure Nat42x Super IO Chipset			
Serial Port A Address	Disabled **3F8/IRQ4** 2F8/IRQ3 3E8/IRQ4 2E8/IRQ3	Allows BIOS to Select Serial Port A Base Addresses.	Option that is used by other serial port is hidden to prevent conflicting settings.
Serial Port B Address	Disabled 3F8/IRQ4 **2F8/IRQ3** 3E8/IRQ4 2E8/IRQ3	Allows BIOS to Select Serial Port B Base Addresses.	Option that is used by other serial port is hidden to prevent conflicting settings.

4.4.2.2.5 USB Configuration Sub-menu

Table 27: BIOS Setup, USB Configuration Sub-menu Selections

Feature	Options	Help Text	Description
USB Configuration			
USB Devices Enabled	N/A	N/A	List of USB devices detected by BIOS.
USB Function	Disabled **Enabled**	Enables USB HOST controllers.	When set to disabled, other USB options are grayed out.
Legacy USB Support	Disabled Keyboard only **Auto** Keyboard and Mouse	Enables support for legacy USB. AUTO option disables legacy support if no USB devices are connected. If disabled, USB Legacy Support will not be disabled until booting an OS.	
Port 60/64 Emulation	**Disabled** Enabled	Enables I/O port 60/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSes.	
USB 2.0 Controller	Disabled **Enabled**	N/A	
USB 2.0 Controller mode	FullSpeed **HiSpeed**	Configures the USB 2.0 controller in HiSpeed (480Mbps) or FullSpeed (12Mbps).	
USB Mass Storage Device Configuration	N/A	Configure the USB Mass Storage Class Devices.	Selects submenu with USB Device enable.

a. USB Mass Storage Device Configuration Sub-menu

Table 28: BIOS Setup, USB Mass Storage Device Configuration Sub-menu Selections

Feature	Options	Help Text	Description
USB Mass Storage Device Configuration			
USB Mass Storage Reset Delay	10 Sec **20 Sec** 30 Sec 40 Sec	Number of seconds POST waits for the USB mass storage device after start unit command.	
Device #1	N/A	N/A	Only displayed if a device is detected, includes a DeviceID string returned by the USB device.
Emulation Type	**Auto** Floppy Forced FDD Hard Disk CDROM	If Auto, USB devices less than 530MB will be emulated as Floppy and remaining as hard drive. Forced FDD option can be used to force a HDD formatted drive to boot as FDD (Ex. ZIP drive).	

Feature	Options	Help Text	Description
Device #n	N/A	N/A	Only displayed if a device is detected, includes a DeviceID string returned by the USB device.
Emulation Type	**Auto** Floppy Forced FDD Hard Disk CDROM	If Auto, USB devices less than 530MB will be emulated as Floppy and remaining as hard drive. Forced FDD option can be used to force a HDD formatted drive to boot as FDD (Ex. ZIP drive).	

4.4.2.2.6 PCI Configuration Sub-menu

This sub-menu provides control over PCI devices and their option ROMs. If the BIOS is reporting POST error 146, use this menu to disable option ROMs that are not required to boot the system.

Table 29: BIOS Setup, PCI Configuration Sub-menu Selections

Feature	Options	Help Text	Description
PCI Configuration			
Onboard Video	Disabled **Enabled**	Enable/Disable on board VGA Controller	
Dual Monitor Video	**Disabled** Enabled	Select which graphics controller to use as the primary boot device. Enabled selects the on board device.	Grayed out if Onboard Video is set to "Disabled."
Onboard NIC 1 (Left)	Disabled **Enabled**		
Onboard NIC 1 ROM	Disabled **Enabled**		Grayed out if device is disabled.
Onboard NIC 2 (Right)	Disabled **Enabled**		
Onboard NIC 2 ROM	Disabled **Enabled**		Grayed out if device is disabled.
Onboard SCSI	Disabled **Enabled**		
Onboard SCSI ROM	Disabled **Enabled**		Grayed out if device is disabled.
Onboard SCSI Mode	**IM/IME** IS	IM/IME = Integrated Mirroring/Integrated Mirroring Enhanced IS = Integrated Striping Before changing modes, back up array data and delete existing arrays, if any. Otherwise, loss of all data may occur.	After OS installation with a selected SCSI RAID mode, only change this mode selection if prepared to rebuild RAID array. Changing the mode could damage current OS installation on RAID volume. Grayed out if device is disabled.

Feature	Options	Help Text	Description
Slot 1 Option ROM	Disabled **Enabled**	PCI-X 64/133	
Slot 2 Option ROM	Disabled **Enabled**	PCI-X 64/133	
Slot 3 Option ROM	Disabled **Enabled**	PCI-X 64/133	Visible only when installed riser supports this slot.
Slot 4 Option ROM	Disabled **Enabled**	PCI-X 64/133	Visible only when installed riser supports this slot.
Slot 5 Option ROM	Disabled **Enabled**	PCI-X 64/133	Visible only when installed riser supports this slot.
Slot 6 Option ROM	Disabled **Enabled**	PCI-X 64/133	Visible only when installed riser supports this slot.

4.4.2.2.7 Memory Configuration Sub-menu

This sub-menu provides information about the DIMMs detected by the BIOS. The DIMM number is printed on the baseboard next to each device.

Table 30: BIOS Setup, Memory Configuration Sub-menu Selections

Feature	Options	Help Text	Description
System Memory Settings			
DIMM 1A	Installed Not Installed Disabled Mirror Spare		Informational display.
DIMM 1B	Installed Not Installed Disabled Mirror Spare		Informational display.
DIMM 2A	Installed Not Installed Disabled Mirror Spare		Informational display.
DIMM 2B	Installed Not Installed Disabled Mirror Spare		Informational display.

Feature	Options	Help Text	Description
DIMM 3A	Installed Not Installed Disabled Mirror Spare		Informational display.
DIMM 3B	Installed Not Installed Disabled Mirror Spare		Informational display.
Extended Memory Test	1 MB 1 KB Every Location **Disabled**	Settings for extended memory test	
Memory Retest	**Disabled** Enabled	If "Enabled", BIOS will activate and retest all DIMMs on the next system boot. This option will automactically reset to "Disabled" on the next system boot.	
Memory Remap Feature	Disabled **Enabled**	Enable: Allow remapping of overlapped PCI memory above the total physical memory. Disable: Do not allow remapping of memory.	
Memory Mirroring / Sparing	**Disabled** Spare Mirror	Disabled provides the most memory space. Sparing reserves memory to replace failures. Mirroring keeps a second copy of memory contents.	Sparing or Mirroring is grayed out if the installed DIMM configuration does not support it.

4.4.2.3 Boot Menu

Table 31: BIOS Setup, Boot Menu Selections

Feature	Options	Help Text	Description
Boot Settings			
Boot Settings Configuration	N/A	Configure settings during system boot.	Selects submenu.
Boot Device Priority	N/A	Specifies the boot device priority sequence.	Selects submenu.
Hard Disk Drives	N/A	Specifies the boot device priority sequence from available hard drives.	Selects submenu.
Removable Drives	N/A	Specifies the boot device priority sequence from available removable drives.	Selects submenu.
CD/DVD Drives	N/A	Specifies the boot device priority sequence from available CD/DVD drives.	Selects submenu.

4.4.2.3.1 Boot Settings Configuration Sub-menu Selections

Table 32: BIOS Setup, Boot Settings Configuration Sub-menu Selections

Feature	Options	Help Text	Description
Boot Settings Configuration			
Quick Boot	Disabled **Enabled**	Allows BIOS to skip certain tests while booting. This will decrease the time needed to boot the system.	
Quiet Boot	Disabled **Enabled** **(this is conflict with previous words in this doc. Based on my memory, it is enabled by default)**	Disabled: Displays normal POST messages. Enabled: Displays OEM Logo instead of POST messages.	
Bootup Num-Lock	**Off** On	Select power-on state for Numlock.	
PS/2 Mouse Support	Disabled Enabled **Auto**	Select support for PS/2 mouse.	
POST Error Pause	Disabled **Enabled**	If enabled, the system will wait for user intervention on critical POST errors. If disabled, the system will boot with no intervention, if possible.	
Hit ‘F2’ Message Display	Disabled **Enabled**	Displays "Press ‘F2’ to run Setup" in POST.	
Scan User Flash Area	**Disabled** Enabled	Allows BIOS to scan the Flash ROM for user binaries.	

4.4.2.3.2 Boot Device Priority Sub-menu Selections

Table 33: BIOS Setup, Boot Device Priority Sub-menu Selections

Feature	Options	Help Text	Description
Boot Device Priority			
1st Boot Device	Varies	Specifies the boot sequence from the available devices. A device enclosed in parenthesis has been disabled in the corresponding type menu.	Number of entries will vary based on system configuration.
nth Boot Device	Varies	Specifies the boot sequence from the available devices. A device enclosed in parenthesis has been disabled in the corresponding type menu.	

4.4.2.3.3 Hard Disk Drive Sub-menu Selections

Table 34: BIOS Setup, Hard Disk Drive Sub-Menu Selections

Feature	Options	Help Text	Description
Hard Disk Drives			
1st Drive	Varies	Specifies the boot sequence from the available devices.	Varies based on system configuration.
nth Drive	Varies	Specifies the boot sequence from the available devices.	Varies based on system configuration.

4.4.2.3.4 Removable Drive Sub-menu Selections

Table 35: BIOS Setup, Removable Drives Sub-menu Selections

Feature	Options	Help Text	Description
Removable Drives			
1st Drive	Varies	Specifies the boot sequence from the available devices.	Varies based on system configuration.
nth Drive	Varies	Specifies the boot sequence from the available devices.	Varies based on system configuration.

4.4.2.3.5 ATAPI CDROM drives sub-menu selections

Table 36: BIOS Setup, CD/DVD Drives Sub-menu Selections

Feature	Options	Help Text	Description
CD/DVD Drives			
1st Drive	Varies	Specifies the boot sequence from the available devices.	Varies based on system configuration.

nth Drive	Varies	Specifies the boot sequence from the available devices.	Varies based on system configuration.

4.4.2.4 Security Menu

Table 37: BIOS Setup, Security Menu Options

Feature	Options	Help Text	Description
Security Settings			
Administrator Password is	N/A	Install / Not installed	Informational display.
User Password is	N/A	Install / Not installed	Informational display.
Set Admin Password	N/A	Set or clear Admin password	Pressing enter twice will clear the password. This option is grayed our when entering setup with a user password.
Set User Password	N/A	Set or clear User password	Pressing enter twice will clear the password.
User Access Level	No Access View Only **Limited** Full Access	LIMITED: allows only limited fields to be changed such as Date and Time. NO ACCESS: prevents User access to the Setup Utility. VIEW ONLY: allows access to the Setup Utility but the fields can not be changed. FULL: allows any field to be changed.	This node is grayed out and becomes active only when Admin password is set.
Clear User Password	N/A	Immediately clears the user password.	Admin uses this option to clear User password (Admin password is used to enter setup is required). This node is gray if Administrator password is not installed.
Fixed disk boot sector protection	**Disabled** Enabled	Enable/Disable Boot Sector Virus Protection.	
Password On Boot	**Disabled** Enabled	If enabled, requires password entry before boot.	This node is grayed out if a user password is not installed.
Secure Mode Timer	**1 minute** 2 minutes 5 minutes 10 minutes 20 minutes 60 minutes 120 minutes	Period of key/PS/2 mouse inactivity specified for Secure Mode to activate. A password is required for Secure Mode to function. Has no effect unless at least one password is enabled.	This node is grayed out if a user password is not installed.
Secure Mode Hot Key (Ctrl-Alt-)	**[L]** [Z]	Key assigned to invoke the secure mode feature. Cannot be enabled unless at least one password is enabled. Can be disabled by entering a new key followed by a backspace or by entering delete.	This node is grayed out if a user password is not installed.

Feature	Options	Help Text	Description
Secure Mode Boot	**Disabled** Enabled	When enabled, allows the host system to complete the boot process without a password. The keyboard will remain locked until a password is entered. A password is required to boot from diskette.	This node is grayed out if a user password is not installed.
Diskette Write Protect	**Disabled** Enabled	Disable diskette write protection when Secure mode is activated. A password is required to unlock the system.	This node is grayed out if a user password is not installed. This node is hidden if the Intel Management Module is not present.
Video Blanking	**Disabled** Enabled	Blank video when Secure mode is activated. A password is required to unlock the system. This option controls the embedded video controller only.	This node is grayed out if a user password is not installed. This node is hidden if the Intel Management Module is not present.
Power Switch Inhibit	**Disabled** Enabled	Disable the Front Panel Power Switch when Secure mode is activated. A password is required to unlock the system.	This node is grayed out if a user password is not installed. This node is hidden if the Intel Management Module is not present.
NMI Control	**Disabled** Enabled	Enable / disable NMI control for the front panel NMI button.	

4.4.2.5 Server Menu

Table 38: BIOS Setup, Server Menu Selections

Feature	Options	Help Text	Description
System management	N/A	N/A	Selects submenu.
Serial Console Features	N/A	N/A	Selects submenu.
Event Log configuration	N/A	Configures event logging.	Selects submenu.
Assert NMI on SERR	Disabled **Enabled**	If enabled, NMI is generated on SERR and logged.	
Assert NMI on PERR	Disabled **Enabled**	If enabled, NMI is generated. SERR option needs to be enabled to activate this option.	Grayed out if “NMI on SERR” is disabled.
Resume on AC Power Loss	**Stays Off** Power On Last State	Determines the mode of operation if a power loss occurs. Stays off, the system will remain off once power is restored. Power On, boots the system after power is restored.	“Last State” is only displayed if the Intel Management Module is present. When displayed, “Last State” is the default. When set to “Stays Off,” “Power Switch Inhibit” is disabled.
FRB-2 Policy	**Disable BSP** Do not disable BSP Retry on Next Boot Disable FRB2 Timer	This controls action if the boot processor will be disabled or not.	“Disable BSP” and “Do not disable BSP” are only displayed if the Intel Management Module is present.

Feature	Options	Help Text	Description
Late POST Timeout	**Disabled** 5 minutes 10 minutes 15 minutes 20 minutes	This controls the time limit for add-in card detection. The system is reset on timeout.	
Hard Disk OS Boot Timeout	**Disabled** 5 minutes 10 minutes 15 minutes 20 minutes	This controls the time limit allowed for booting an operating system from a Hard disk drive. The action taken on timeout is determined by the OS Watchdog Timer policy setting.	
PXE OS Boot Timeout	**Disabled** 5 minutes 10 minutes 15 minutes 20 minutes	This controls the time limit allowed for booting an operating system using PXE boot. The action taken on timeout is determined by OS Watchdog Timer policy setting.	
OS Watchdog Timer Policy	**Stay On** Reset Power Off	Controls the policy upon timeout. Stay on action will take no overt action. Reset will force the system to reset. Power off will force the system to power off.	
Platform Event Filtering	Disabled **Enabled**	Disable trigger for system sensor events.	

4.4.2.5.1 System Management Sub-menu Selections

Table 39: BIOS Setup, System Management Sub-menu Selections

Feature	Options	Help Text	Description
Server Board Part Number	N/A	N/A	Field contents varies
Server Board Serial Number	N/A	N/A	Field contents varies
NIC 1 MAC Address	N/A	N/A	Field contents varies
NIC 2 MAC Address	N/A	N/A	Field contents varies
System Part Number	N/A	N/A	Field contents varies
System Serial Number	N/A	N/A	Field contents varies
Chassis Part Number	N/A	N/A	Field contents varies
Chassis Serial Number	N/A	N/A	Field contents varies
BIOS Version	N/A	N/A	BIOS ID string (excluding the build time and date).
BMC Device ID	N/A	N/A	Field contents varies
BMC Firmware Revision	N/A	N/A	Field contents varies
BMC Device Revision	N/A	N/A	Field contents varies
PIA Revision	N/A	N/A	Field contents varies
SDR Revision	N/A	N/A	Field contents varies
HSC FW Revision (HSBP)	N/A	N/A	Firmware revision of the Hot-swap controller. Displays n/a if the controller is not present.

4.4.2.5.2 Serial Console Features Sub-menu Selections

Table 40: BIOS Setup, Serial Console Features Sub-menu Selections

Feature	Options	Help Text	Description
Serial Console Features			
BIOS Redirection Port	**Disabled** Serial A Serial B	If enabled, BIOS uses the specified serial port to redirect the console to a remote ANSI terminal. Enabling this option disables Quiet Boot.	When the Intel Management Module is present, the help text directs the user to select Serial B for Serial Over LAN.
		If enabled, BIOS uses the specified serial port to redirect the console to a remote ANSI terminal. Enabling this option disables Quiet Boot. For Serial Over LAN, select Serial B.	
Baud Rate	9600 **19.2K** 38.4K 57.6K 115.2K	N/A	
Flow Control	No Flow Control **CTS/RTS** XON/XOFF CTS/RTS + CD	If enabled, it will use the Flow control selected. CTS/RTS = Hardware XON/XOFF = Software CTS/RTS + CD = Hardware + Carrier Detect for modem use.	
Terminal Type	PC-ANSI **VT100+** VT-UTF8	VT100+ selection only works for English as the selected language. VT-UTF8 uses Unicode. PC-ANSI is the standard PC-type terminal.	
ACPI Redirection port	**Disabled** Serial A Serial B	Enable / Disable the ACPI OS Headless Console Redirection.	
Serial Port Connector	Serial A **Serial B**	Selects which serial port will be routed to the serial port connector on the back of the chassis. Serial A selects UARTA and Serial B selects UARTB.	

4.4.2.5.3 Event Log Configuration Sub-menu Selections

Table 41: BIOS Setup, Event Log Configuration Sub-menu Selections

Feature	Options	Help Text	Description
Event Log Configuration			
Clear All Event Logs	**Disabled** Enabled	Setting this to Enabled will clear the System Event Log during the next boot.	

Feature	Options	Help Text	Description
BIOS Event Logging	Disabled **Enabled**	Select enabled to allow logging of BIOS events.	Enables BIOS to log events to the SEL. This option controls BIOS events only.
Critical Event Logging	Disabled **Enabled**	If enabled, BIOS will detect and log events for system critical errors. Critical errors are fatal to system operation. These errors include PERR, SERR, ECC.	Enable SMM handlers to detect and log events to SEL.
ECC Event Logging	Disabled **Enabled**	Enables or Disables ECC Event Logging.	Grayed out if "Critical Event Logging" option is disabled.
PCI Error Logging	Disabled **Enabled**	Enables or Disables PCI Error Logging.	Grayed out if "Critical Event Logging" option is disabled.
FSB Error Logging	Disabled **Enabled**	Enables or Disables Front-Side Bus Error Logging.	Grayed out if "Critical Event Logging" option is disabled.
Hublink Error Logging	Disabled **Enabled**	Enables or Disables Hublink Error Logging.	Grayed out if "Critical Event Logging" option is disabled.

4.4.2.6 Exit Menu

Table 42: BIOS Setup, Exit Menu Selections

Feature	Options	Help Text
Exit Options		
Save Changes and Exit	N/A	Exit system setup after saving the changes. F10 key can be used for this operation.
Discard Changes and Exit	N/A	Exit system setup without saving any changes. ESC key can be used for this operation.
Discard Changes	N/A	Discards changes done so far to any of the setup questions. F7 key can be used for this operation.
Load Setup Defaults	N/A	Load Setup Default values for all the setup questions. F9 key can be used for this operation.
Load Custom Defaults	N/A	Load custom defaults.
Save Custom Defaults	N/A	Save custom defaults

4.5 Rolling BIOS and On-line Updates

The Online Update nomenclature refers to the ability to update the BIOS while the server is online and in operation, as opposed to taking the server out of operation while performing a BIOS update. The rolling BIOS nomenclature refers to the capability of having two copies of BIOS: the current one in use, and a second BIOS 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 BIOS relies on specialized hardware and additional flash space to accomplish online update/rolling of the BIOS. To this end, the flash is divided into two partitions, primary and secondary. The active partition from which the system boots shall be referred to as the primary partition. The AMI FLASH update suite and Intel Online updates preserve the existing BIOS image on the primary partition. BIOS updates are diverted to the secondary partition. After the update is complete, a notification flag is set. During the subsequent boot following the BIOS update, the system continues to attempt to boot from the primary BIOS partition. On determining that a BIOS update occurred in the previous boot, the system then attempts to boot from the new BIOS. If a failure happens while booting to the new BIOS, the specialized hardware on the system switches back to the primary BIOS partition, thus affecting a “Roll Back”.

4.5.1 Flash Update Utility

Server platforms support a DOS-based firmware update utility. This utility loads a fresh copy of the BIOS into the flash ROM.

The BIOS update may affect the following items:

- The system BIOS, including the recovery code, setup utility and strings.
- Onboard video BIOS, SCSI BIOS, and other option ROMS for the devices embedded on the server board.
- OEM binary area.
- Microcode updates.

4.5.1.1 Flash BIOS

An `afuXXX` AMI Firmware Update utility (such as `afudos`, `AFUWIN`, `afulnx`, or `AFUEFI`) is required for a BIOS update.

4.5.1.2 User Binary Area

The baseboard includes an area in flash for implementation-specific OEM add-ons. This OEM binary area can be updated as part of the system BIOS update or it can be updated independent of the system BIOS.

4.5.1.3 Recovery Mode

Three conditions can cause the system to enter recovery mode:

- Pressing a hot key
- Setting the recovery jumper (J1H2, labeled RCVR BOOT) to pins 2-3
- Damaging the ROM image, which will cause the system to enter recovery and update the system ROM without the boot block.

4.5.1.4 BIOS Recovery

The BIOS has a ROM image size of 2 MB. A standard 1.44MB floppy diskette cannot hold the entire ROM file due to the large file size. To compensate for this, a Multi-disk recovery method is available for BIOS recovery.

The BIOS contains a primary and secondary partition, and can support rolling BIOS updates. The recovery process performs an update on the secondary partition in the same fashion that the normal flash update process updates the secondary partition. After recovery is complete and the power is cycled to the system, the BIOS partitions switch and the code executing POST will be the code that was just flashed from the recovery media. The BIOS is made up of a boot block recovery section, a main BIOS section, an OEM logo/user binary section, and an NVRAM section. The NVRAM section will either be preserved or destroyed based on a hot key press during invocation of the recovery. All the other sections of the secondary BIOS will be updated during the recovery process. If an OEM wishes to preserve the OEM section across an update, it is recommended that the OEM modify the provided `AMIBOOT.ROM` file with the user binary or OEM logo tools before performing the recovery.

A BIOS recovery can be accomplished from one of the following devices: a standard 1.44 or 2.88 MB floppy drive, an USB Disk-On-Key, an ATAPI CD-ROM/DVD, an ATAPI ZIP drive, or a LS-120/LS-240 removable drive.

The recovery media must include the BIOS image file, `AMIBOOT.ROM`.

The recovery mode procedure is as follows:

1. Insert or plug-in the recovery media with the `AMIBOOT.ROM` file.

2. Power on the system. When progress code E9 is displayed on port 80h, the system will detect the recovery media (if there is no image file present, the system will cycle through progress code F1 to EF).

3. When F3 is displayed on port 80h, the system will read the BIOS image file.

Note: Three different hot-keys can be invoked:

- <Ctrl+Home> - Recovery with CMOS destroyed and NVRAM preserved.
- <Ctrl+PageDown> - Recovery with both CMOS and NVRAM preserved.
- <Ctrl+PageUp> - Recovery with both CMOS and NVRAM destroyed.

4.5.2 .Configuration Reset

Setting the Clear CMOS jumper (board location J1H2 jumper Row ‘C’) produces a “reset system configuration” request. When a request is detected, the BIOS loads the default system configuration values during the next POST.

In systems configured with an Intel Management Module, the CMOS can be cleared without opening the chassis. Using the control panel, the user can hold the reset button for 4 seconds and then press the power button while still pressing the reset button. In addition, IMM give the capability of having software issue a “reset system configuration” request. Software can send a specific OEM command to the Sahalee BMC to indicate the request.

4.6 OEM Binary

System customers can supply 16 KB of code and data for use during POST and at run-time. Individual platforms may support a larger user binary. User binary code is executed at several defined hook points during POST.

The user binary code is stored in the system flash. If no run-time code is added, the BIOS temporarily allocates a code. If run-time code is present, the BIOS shadows the entire block as though it were an option ROM. The BIOS leaves this region writeable to allow the user binary to update any data structures it defines. System software can locate a run-time user binary by searching for it like an option ROM. The system vendor can place a signature within the user binary to distinguish it from other option ROMs. Refer to the SE7520JR2 BIOS EPS for further details.

4.7 Security

The BIOS provides a number of security features. This section describes the security features and operating model.

The BIOS uses passwords to prevent unauthorized tampering with the system. Once secure mode is entered, access to the system is allowed only after the correct password(s) has been entered. Both user and administrator passwords are supported by the BIOS. To set a user password, an administrator password must be entered during system configuration using the BIOS setup menu. The maximum length of the password is seven characters. The password cannot have characters other than alphanumeric (a-z, A-Z, 0-9).

Once set, a password can be cleared by entering the password change mode and pressing enter twice without inputting a string. All setup fields can be modified when entering the administrator password. The “user access level” setting in the BIOS setup Security menu controls the user access level. The administrator can choose “No Access” to block the user from accessing any setup features. “Limited Access” will allow only the date/time fields and the user password to be changed. “View Only” allows the user to enter BIOS setup, but not change any settings.

Administrator has control over all fields in the setup, including the ability to clear the user password.

If the user enters three wrong passwords in a row during the boot sequence, the system will be placed into a halt state. This feature makes it difficult to break the password by “trial and error.”

The BIOS Setup may provide an option for setting the EMP password. However, the EMP password is only utilized by the mBMC; this password does not affect the BIOS security in any way, nor does the BIOS security engine provide any validation services for this password. EMP security is handled primarily through the mBMC and EMP utilities.

4.7.1 Operating Model

The following table summarizes the operation of security features supported by the BIOS.

Some security features require the Intel Management Module (IMM) to be installed. These include “Diskette Write Protect”, “Video Blanking”, and “Power Switch inhibit.”

Table 43: Security Features Operating Model

Mode	Entry Method/ Event	Entry Criteria	Behavior	Exit Criteria	After Exit
Secure boot	Power On/Reset	User Password and Secure Boot Enabled	Prompts for password if booting from drive A. Enters secure mode just before scanning option ROMs as indicated by flashing LEDs on the keyboard. Disables the NMI switch on the front panel if enabled in Setup. Accepts no input from PS/2 mouse or PS/2 keyboard; however, the Mouse driver is allowed to load before a password is required. If booting from drive A and the user enters correct password, the system boots normally. If the IMM module is installed and the options are enabled in Setup, the system also blanks on-board video, disables floppy writes, and disables the power and reset switches on the front panel.	User Password Admin Password	Floppy writes are re-enabled. Front panel switches are re-enabled. PS/2 Keyboard and PS/2 mouse inputs are accepted. System attempts to boot from drive A. If the user enters correct password, and drive A is bootable, the system boots normally
Password on boot	Power On/Reset	User Password set and password on boot enabled and Secure Boot Disabled in setup	System halts for user Password before scanning option ROMs. The system is not in secure mode. No mouse or keyboard input is accepted except the password.	User Password Admin Password	Front Panel switches are re-enabled. PS/2 Keyboard and PS/2 mouse inputs are accepted. The system boots normally. Boot sequence is determined by setup options.
Fixed disk boot sector	Power On/Reset	Set feature to Write Protect in Setup	Will write protect the master boot record of the IDE hard drives only if the system boots from a floppy. The BIOS will also write protect the boot sector of the drive C: if it is an IDE drive.	Set feature to Normal in Setup	Hard drive will behave normally.

Administrator/User Passwords and F2 Setup Usage Model
Notes:

- Visible=option string is active and changeable
- Hidden=option string is inactive and not visible
- Shaded=option string is gray-out and view-only

There are three possible password scenarios:

Scenario #1

Administrator Password Is Not Installed User Password Is Not Installed
Login Type: N/A
Set Admin Password (visible) Set User Password (visible) User Access Level [Full]** (shaded) Clear User Password (hidden)

** User Access Level option will be Full and Shaded as long as the administrator/supervisor password is not installed.

Scenario #2

Administrator Password Is Installed User Password Is Installed
Login Type: Admin/Supervisor
Set Admin Password (visible) Set User Password (visible) User Access Level [Full] (visible) Clear User Password (visible)
Login Type: User
Set Admin Password (hidden) Set User Password (visible) User Access Level [Full] (Shaded) Clear User Password (hidden)

Scenario #3

Administrator Password Is Installed User Password Is Not Installed
Login Type: Supervisor
Set Admin Password (visible)

Set User Password (visible) User Access Level [Full] (visible) Clear User Password (hidden)
Login Type: <Enter>
Set Admin Password (hidden) Set User Password (visible) User Access Level [Full] (Shaded) Clear User Password (hidden)

4.7.2 Password Clear Jumper

If the user or administrator password(s) is lost or forgotten, moving the password clear jumper (board location J1H3) to the clear position will clear both passwords. The BIOS determines if the password clear jumper is in the clear position during BIOS POST and clears any passwords if present. The password clear jumper must be restored to its original position before a new password(s) can be set.

4.8 Extensible Firmware Interface (EFI)

When EFI is selected as a boot option, the BIOS will support an EFI Specification 1.10 compliant environment. More details on EFI are available at http://developer.intel.com/technology/efi/index.htm

4.8.1 EFI Shell

The EFI Shell is a special type of EFI application that allows EFI commands and other EFI applications to be launched. The BIOS implements an EFI shell in flash and the shell can be invoked from the BIOS provided EFI environment. The EFI shell provided in flash implements all the commands specified in the `EFI1.1ShellCommands.pdf` document that comes with the EFI sample implementation, revision 1.10.14.62 (available from http://developer.intel.com/technology/efi/main_sample.htm).

4.9 Operating System Boot, Sleep, and Wake

The IPMI 1.5 specification, chapter 22.10 and 22.11, has provisions for server management devices to set certain boot parameters by setting boot flags. Among the boot flags, which are parameter #5 in the IPMI specification, the BIOS checks data 1-3 for forced boot options.

The BIOS supports force boots from: PXE, HDD, FDD, and CD.

On each boot, the BIOS determines what changes to boot options have been set by invoking the Get System Boot Options Command, takes appropriate action, and clears these settings.

4.9.1 Microsoft* Windows* Compatibility

Intel Corporation and Microsoft Corporation co-author design guides for system designers using Intel® processors and Microsoft* operating systems. These documents are updated yearly to address new requirements and current trends.

PC200x specifications are intended for systems that are designed to work with Windows 2000* and Windows XP* class operating systems. The Hardware Design Guide (HDG) for the Windows XP platform is intended for systems that are designed to work with Windows XP class operating systems. Each specification classifies the systems further and has requirements based on the intended usage for that system. For example, a server system that will be used in small home/office environments has different requirements than one used for enterprise applications. The BIOS supports HDG 3.0.

4.9.2 Advanced Configuration and Power Interface (ACPI)

The BIOS is ACPI 2.0c compliant. The primary role of the BIOS is to provide ACPI tables. During POST, the BIOS creates the ACPI tables and locates them in extended memory (above 1MB). The location of these tables is conveyed to the ACPI-aware operating system through a series of tables located throughout memory. The format and location of these tables is documented in the publicly available ACPI specification.

To prevent conflicts with a non-ACPI-aware operating system, the memory used for the ACPI tables is marked as “reserved”.

As described in the ACPI specification, an ACPI-aware operating system generates an SMI to request that the system be switched into ACPI mode. The BIOS responds by setting up all system (chipset) specific configuration required to support ACPI, and sets the SCI_EN bit as defined by the ACPI specification. The system automatically returns to legacy mode on hard reset or power-on reset.

The BIOS supports S0, S1, S4, and S5 states. S1 and S4 are considered sleep states. The ACPI specification defines the sleep states and requires the system to support at least one of them.

While entering the S4 state, the operating system saves the context to the disk and most of the system is powered off. The system can wake on a power button press, or a signal received from a wake-on-LAN compliant LAN card (or onboard LAN), modem ring, PCI power management interrupt, or RTC alarm. The BIOS performs complete POST upon wake up from S4, and initializes the platform.

The system can wake from the S1 state using a PS/2 keyboard, mouse, or USB device, in addition to the sources described above.

The wake-up sources are enabled by the ACPI operating systems with cooperation from the drivers; the BIOS has no direct control over the wakeup sources when an ACPI operating system is loaded. The role of the BIOS is limited to describing the wakeup sources to the operating system and controlling secondary control/status bits via the DSDT table.

The S5 state is equivalent to operating system shutdown. No system context is saved.

4.9.2.1 Sleep and Wake Functionality

The BIOS supports a control panel power button. The power button is a request that is forwarded by the mBMC to the ACPI power state machines in the chipset. It is monitored by the mBMC and does not directly control power on the power supply.

The BIOS supports a control panel sleep button. The sleep button may not be provided on all control panel designs. On systems where the sleep button is optional, a system configuration option will be provided to enable or disable the sleep button. The ACPI tables will be updated to indicate the presence or absence of the sleep button. Removal of the sleep button does not prevent an ACPI OS from entering a sleep state.

The sleep button has no effect unless an operating system is running. If the OS is running, pressing the sleep button causes an event. The OS will cause the system to transition to the appropriate ACPI system state depending on the current user settings.

The platform supports a control panel reset button. The reset button is a request that is forwarded by the mBMC to the chipset. The BIOS does not affect the behavior of the reset button.

The BIOS supports a control panel NMI button. The NMI button may not be provided on all control panel designs. The NMI button is a request that causes the mBMC to generate an NMI (non-maskable interrupt). The NMI is captured by the BIOS during Boot Services time or the OS during Runtime. The BIOS will simply halt the system upon detection of the NMI.

4.9.2.2 Power Switch Off to On

The chipset may be configured to generate wakeup events for several different system events: Wake on LAN, PCI Power Management Interrupt (PMI), and Real Time Clock Alarm are examples of these events. The operating system will program the wake sources before shutdown. A transition from either source results in the mBMC starting the power-up sequence. Since the processors are not executing, the BIOS does not participate in this sequence. The hardware receives power good and reset from the mBMC and then transitions to an ON state.

4.9.2.3 On to Off (OS absent)

The SCI interrupt is masked. The firmware polls the power button status bit in the ACPI hardware registers and sets the state of the machine in the chipset to the OFF state. The mBMC monitors power state signals from the chipset and de-asserts PS_PWR_ON to the power supply. As a safety mechanism, the mBMC automatically powers off the system in 4-5 seconds if the BIOS fails to service the request.

4.9.2.4 On to Off (OS present)

If an operating system is loaded, the power button generates a request (via SCI) to the OS to shutdown the system. The OS retains control of the system and OS policy determines what sleep state (if any) the system transitions into.

4.9.2.5 On to Sleep (ACPI)

If an operating system is loaded, the sleep button generates a request (via SCI) to the OS to place the system in “sleep” mode. The OS retains control of the system and OS policy determines what sleep state (if any) the system transitions into.

4.9.2.6 Sleep to On (ACPI)

If an operating system is loaded, the sleep button generates a wake event to the ACPI chipset and a request (via SCI) to the OS to place the system in the “On” state. The OS retains control of the system and OS policy determines what sleep state (if any) and sleep sources the system can wake from.

4.9.2.7 System Sleep States

The platform supports the following ACPI System Sleep States:

- ACPI S0 (working) state
- ACPI S1 (sleep) state
- ACPI S4 (suspend to disk) state
- ACPI S5 (soft-off) state

The platform supports the following wake up sources in an ACPI environment. As noted above, the OS controls the enabling and disabling of these wake sources.

- Devices that are connected to all USB ports, such as USB mice and keyboards can wake the system up from the S1 sleep state.
- PS/2 keyboards and mice can wake up the system from the S1 sleep state.
- Both serial ports can be configured to wake up the system from the S1 sleep state.
- PCI cards, such as LAN cards, can wake up the system from the S1 or S4 sleep state. Note that the PCI card must have the necessary hardware for this to work.
- As required by the ACPI Specification, the power button can always wake up the system from the S1 or S4 state.

2.

Additionally, if an ACPI operating system is loaded, the following can cause the system to wake up: the PME, RTC, or Wake-On-LAN.

Table 44: Supported Wake Events

Wake Event	Supported via ACPI (by sleep state)	Supported Via Legacy Wake
Power Button	Always wakes system.	Always wakes system
Ring indicate from Serial A	Wakes from S1 and S4.	Yes
Ring indicate from Serial B	Wakes from S1 and S4. If Serial-B (COM2) is used for Emergency Management Port, Serial-B wakeup is disabled.	Yes
PME from PCI cards	Wakes from S1 and S4.	Yes
RTC Alarm	Wakes from S1. Always wakes the system up from S4.	No
Mouse	Wakes from S1.	No
Keyboard	Wakes from S1.	No
USB	Wakes from S1.	No

4.10 PXE BIOS Support

The BIOS will support PXE-compliant implementations that:

- Locate and configure all PXE-capable boot devices (UNDI Option ROMs) in the system, both built-in and add-ins.
- Supply a PXE according to the specification if the system includes a built-in network device.
- Meet the following specifications: System Management BIOS (SMBIOS) Reference Specification v2.2 or later. The requirements defined in Sections 3 and 4 of the BIOS Boot Specification (BBS) v1.01or later, to support network adapters as boot devices. Also, supply a valid UUID and Wake-up Source value for the system via the SMBIOS structure table.

4.11 Console Redirection

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

The BIOS will take the Setup values for Serial console redirection and map them to the ACPI SPCR tables. The BIOS setup tokens for serial console will also read the BMC serial console values to sync up.

Text-based console redirection is also supported over the Serial Over LAN (SOL) protocol. SOL is built on top of the IPMI-over-LAN infrastructure specified in the IPMI 2.0 specification. When the SOL feature is activated by establishing a LAN connection to the BMC and activating the SOL to be enabled, the EMP-based connectivity is disabled.

The IMM uses UDP datagrams to send SOL character data as “SOL Messages”. The “SOL Messages” packet format follows that used for IPMI-over-LAN with extensions to support SOL Messages as a new message type. SOL requires the support of the VT/UTF-8 character set specified in the Microsoft* Windows.Net* headless requirements from Microsoft. The application displaying SOL data must be VT/UTF-8 aware. The console sends keystrokes in a UDP packet to the server.

If the session ID of SOL matches the session ID in boot block info, then the BIOS starts serial-based redirection services. If the session IDs do not match, the BIOS follows the path specified in the IPMI section and launches LAN or serial console redirection services.

BIOS Console redirection terminates before giving control to an operating system. The operating system is responsible for continuing the Console Redirection after that point. BIOS console redirection is a text-based console and any graphical data, such as a logo, is not redirected.

BIOS Console Redirection is intended to accomplish the implementation of VT-UTF8 console redirection support in Intel® server BIOS products. That implementation will meet the functional requirements set forth in the Microsoft Whistler WHQL requirements for headless operation of servers, as well as maintain a necessary degree of backward compatibility with existing Intel server BIOS products, and meet the architectural requirements of Intel server products currently in development.

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.

If the BIOS determines that console redirection is enabled, it will read the current baud rate and pass this value to the appropriate management controller via the IPMB. Through the redirection capabilities of the BMC on Intel® platforms, this serial port UART input/output stream is further redirected and sent over a platform LAN device as a packetized serial-byte stream. This BMC function is called Serial over LAN, or SOL, and further optimizes space requirements and server management capability. SOL is only supported by the IMM.

5. Platform Management

The Platform Management sub-system on the Server Board SE7520JR2 consists of a micro-controller, communication buses, sensors, system BIOS, and server management firmware. It provides for three different levels of platform management: On-Board Platform Instrumentation based around the National Semiconductor* PC87431M mini-Baseboard Management Controller (mBMC), the Intel® Management Module Professional Edition, and the Intel® Management Module Advanced Edition, which are based on Intel’s “Sahalee” BMC. As shipped, the baseboard comes standard with On-Board Platform Instrumentation. A 120-pin connector on the baseboard provides the interface to the optionally installed Intel Management Modules (IMM).

The following table summarizes the supported features for each management level:

Table 45: Suppoted Management Features by Tier

Element	On-Board Platform Instrumentation	Intel® Management Module - Professional Edition	Intel® Management Module - Advanced Edition
IPMI Messaging, Commands, and Abstractions	Yes	Yes	Yes
Baseboard Management Controller (BMC)	Yes	Yes	Yes
Sensors	Limited	Yes	Yes
Sensor Data Records (SDRs) and SDR Repository	Limited	Yes	Yes
FRU Information	Limited	Yes	Yes
Autonomous Event Logging	Yes	Yes	Yes
System Event Log (SEL)	92 Entries	3276 Entries	3276 Entries
BMC Watchdog Timer, covering BIOS and run-time software	Limited	Yes	Yes

Element	On-Board Platform Instrumentation	Intel® Management Module - Professional Edition	Intel® Management Module - Advanced Edition
IPMI Channels, and Sessions	Limited	Yes	Yes
EMP (Emergency Management Port) - IPMI Messaging over Serial/Modem. This feature is also referred to as DPC (Direct Platform Control) over serial/modem.	No	Yes	Yes
Serial/Modem Paging	No	Yes	Yes
Serial/Modem Alerting over PPP using the Platform Event Trap (PET) format	No	Yes	Yes
DPC (Direct Platform Control) - IPMI Messaging over LAN (available via both on-board network controllers)	Yes	Yes	Yes
LAN Alerting using PET	Yes	Yes	Yes
Platform Event Filtering (PEF)	Yes	Yes	Yes
ICMB (Intelligent Chassis Management Bus) - IPMI Messaging between chassis	No	Yes	Yes
PCI SMBus support	No	Yes	Yes
Fault Resilient Booting	Limited	Yes	Yes
BIOS logging of POST progress and POST errors	Errors Only	Yes	Yes
Integration with BIOS console redirection via IPMI v2.0 Serial Port Sharing	No	Yes	Yes
Access via web browser	No	No	Yes
SNMP access	No	No	Yes
Telnet access	No	No	Yes
DNS support	No	No	Yes
DHCP support (dedicated NIC only)	No	No	Yes
Memory Sparing/Mirroring sensor support	No	Yes	Yes
Alerting via Email	No	No	Yes
Keyboard, Video, Mouse (KVM) redirection via LAN	No	No	Yes
High speed access to dedicated NIC	No	No	Yes

This chapter will provide an overview of the On-board Platform Instrumentation architecture and details of it features and functionality including BIOS interactions and support. Refer to the Technical Product Specification for the Professional and Advanced modules for detailed description of their features and functionality.

Note: The generic term “BMC” may be used throughout this section when a feature and/or function being described is common to both the mBMC and the Sahalee BMC. If a described feature or function is unique, the specific management controller will be referenced.

5.1 Platform Management Architecture Overview

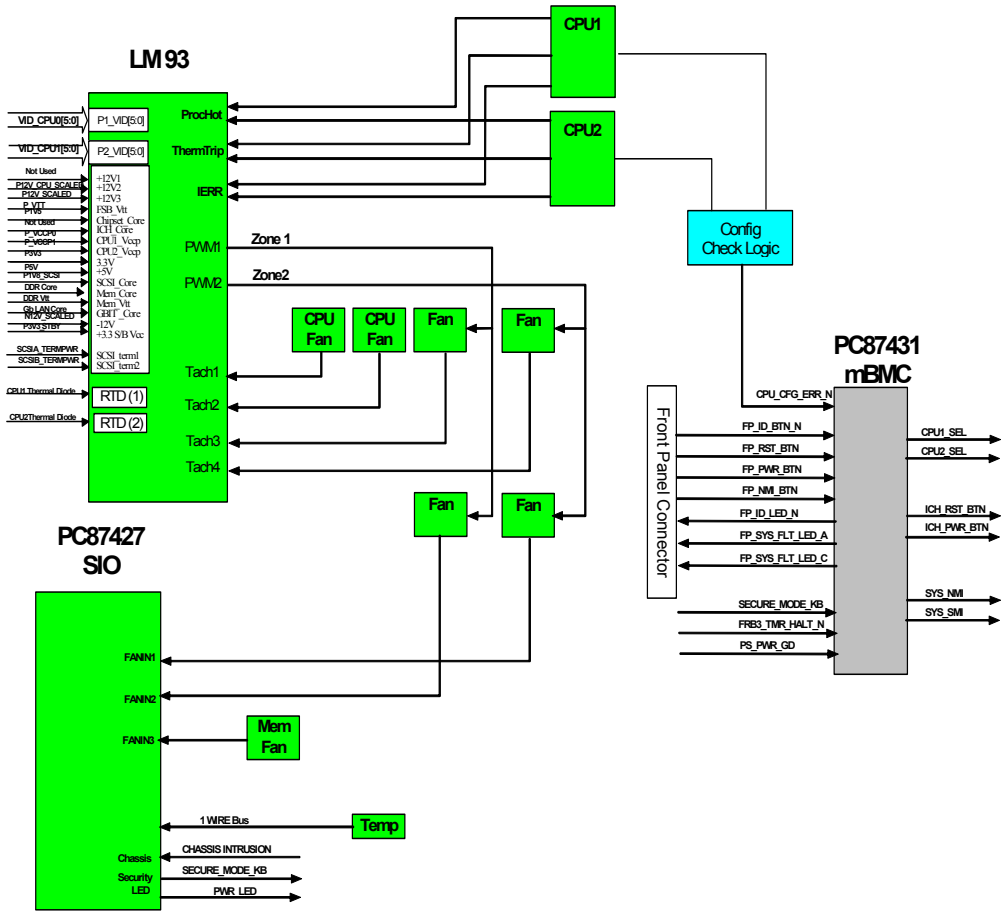


Figure 19. On-Board Platform Management Architecture

5.1.1 5V Standby

The power supply must provide a 5V Standby power source for the platform to provide any management functionality. 5V Standby is a low power 5V supply that is active whenever the system is plugged into AC power. 5V Standby is used by the following onboard management devices:

- Management Controller (BMC and/or mBMC) and associated RAM, Flash, and SEEPROM which are used to monitor the various system power control sources including the front panel Power Button, the baseboard RTC alarm signal, and power on request messages from the auxiliary IPMB connector and PCI SMBus.
- On-board NICs that support IPMI-over-LAN and LAN Alerting, Wake-On LAN, and Magic Packet* operation.
- Emergency management port
- IPMB
- PCI SMBus in addition to certain logic and private busses used for power control
- ICMB Transceiver card (if present)
- IPMB isolation circuit
- System Status LED on the front panel
- System Identify LED

5.1.2 IPMI Messaging, Commands, and Abstractions xxx

The IPMI specification defines a standardized, abstracted, message-based interface between software and the platform management subsystem, and a common set of messages (commands) for performing operations such as accessing temperature, voltage, and fan sensors, setting thresholds, logging events, controlling a watchdog timer, etc.

IPMI also includes a set of records called Sensor Data Records (SDRs) that make the platform management subsystem self-descriptive to system management software. The SDRs include software information such as how many sensors are present, what type they are and what events they generate. The SDRs also include information such as minimum and maximum ranges, sensor type, accuracy and tolerance, etc., that guides software in interpreting and presenting sensor data.

Together, IPMI Messaging and the SDRs provide a self-descriptive, abstracted platform interface that allows management software to automatically configure itself to the number and types of platform management features on the system. In turn, this enables one piece of management software to be used on multiple systems. Since the same IPMI messages are used over the serial/modem and LAN interfaces, a software stack designed for in-band (local) management access can readily be re-used as an out-of-band remote management stack by changing the underlying communications layer for IPMI messaging.

5.1.3 IPMI 'Sensor Model'

An IPMI-compatible 'Sensor Model' is used to unify the way that temperature, voltage, and other platform management status and control is represented and accessed. The implementation of this model is done according to command and data formats defined in the *Intelligent Platform Management Interface Specification.*

The majority of monitored platform elements are accessed as logical 'Sensors' under this model. This access is accomplished using an abstracted, message-based interface (IPMI messages). Instead of having system software access the platform monitoring and control hardware registers directly, it sends commands, such as the *Get Sensor Reading* command, for sensor access. The message-based interface isolates software from the particular hardware implementation.

System Management Software discovers the platform's sensor capabilities by reading the Sensor Data Records from a Sensor Data Record Repository managed by the management controller. Sensor Data Records provide a list of the sensors, their characteristics, location, type, and associated Sensor Number, for sensors in a particular system. The Sensor Data Records also hold default threshold values (if the sensor has threshold based events), factors for converting a sensor reading into the appropriate units (mV, rpm, degrees Celsius, etc.), and information on the types of events that a sensor can generate.

Sensor Data Records also provide information on where Field Replaceable Unit (FRU) information is located, and information to link sensors with the entity and/or FRU they're associated with.

Information in the SDRs is also used for configuring and restoring sensor thresholds and event generation whenever the system powers up or is reset. This is accomplished via a process called the 'initialization agent'. The BMC reads the SDRs and based on bit settings, writes the threshold data. Then it enables event generation for the various sensors it monitors and in management controllers on the IPMB for systems based on the Standard or Advanced management models.

System Management Software uses the data contained in the Sensor Data Record information to locate sensors in order to poll them, interpret, and present their data readings, adjust thresholds, interpret SEL entries, and alter event generation settings.

In Professional and Advanced management models, SDRs also provide a mechanism for extending the baseboard management with additional chassis or OEM 'value-added' monitoring and events. The baseboard monitoring can be extended by implementing an IPMI-compatible management controller, connecting it to the IPMB, and adding new SDRs describing that controller and its sensors to the SDR Repository. System Management Software can then read the SDRs and use them to automatically incorporate the additional sensors.

5.1.4 Private Management Busses

A 'Private Management Bus' is a single-master I^2C bus that is controlled by the management controller. Access to any of the devices on the Private Management Bus is accomplished indirectly via commands to the management controller via the IPMB or system interfaces. Private Management busses are a common mechanism used for accessing temperature sensors, system processor information, and other baseboard monitoring devices that are located in various locations in the system.

The devices on the Private Management Bus are isolated from traffic on the IPMB. Since devices such as temperature sensors are polled by the management controller, this gets the polling traffic off the 'public' IPMB bus. This also increases the reliability of access to the information, since issues with IPMB bus arbitration and message retries are avoided.

Furthermore, placing managed I^2C devices on the private management bus frees up the I^2C addresses that those devices would have used up on the IPMB.

5.1.5 Management Controllers

At the heart of platform management is a management controller. To support the tiered management model, the Server Board SE7520JR2 supports two different management controllers, the PC87431M mini-Baseboard Management Controller (mBMC) from National Semiconductor* and Intel's Sahalee BMC. The Professional and Advanced modules electrically replace the mBMC with the more full featured 'Sahalee' microcontroller. Sahalee is a custom ARM7-TDMI based microcontroller designed for baseboard management applications on Intel Server baseboards.

The management controller is a microcontroller that provides the intelligence at the heart of the Intelligent Platform Management architecture. The primary purpose of the management controller is to autonomously monitor system 'sensors' for system platform management events, such as over-temperature, out-of-range voltages, etc., and log their occurrence in the non-volatile System Event Log (SEL). This includes events such as over-temperature and over-voltage conditions, fan failures, etc. The management controller also provides the interface to the sensors and SEL so System Management Software can poll and retrieve the present status of the platform. The contents of the log can be retrieved 'post mortem' in order provide failure analysis information to field service personnel. It is also accessible by System Management Software, such as Intel Server Management (ISM), running under the OS.

The management controller includes the ability to generate a selectable action, such as a system power-off or reset, when a match occurs to one of a configurable set of events. This capability is called *Platform Event Filtering,* or PEF.

The management controller includes 'recovery control' functions that allow local or remote software to request actions such as power on/off, power cycle, and system hard resets, plus an IPMI Watchdog Timer that can be used by BIOS andr run-time management software as a way to detect software hangs.

The management controller provides 'out-of-band' remote management interfaces providing access to the platform health, event log, and recovery control features via LAN (all tiers). IMM based systems also allow access via serial/modem, IPMB, PCI SMBus, and ICMB interfaces.

These interfaces remain active on standby power, providing a mechanism where the SEL, SDR, and recovery control features can be accessed even when the system is powered down.

Because the management controller operates independently from the main processor(s), the management controller monitoring and logging functions, and the out-of-band interfaces can remain operative even under failure conditions that cause the main processors, OS, or local system software to stop.

The management controller also provides the interface to the non-volatile 'Sensor Data Record (SDR) Repository'. IPMI Sensor Data Records provide a set of information that system management software can use to automatically configure itself for the number and type of IPMI sensors (e.g. temperature sensors, voltage sensors, etc.) in the system. This information allows management software to automatically adapt itself to the particular system, enabling the development of management software that can work on multiple platforms without requiring the software to be modified.

The following is a list of the major functions that are managed by either or both the mBMC and Sahalee BMC.

- Sensors and Sensor Polling
- FRU Information Access. FRU (Field Replaceable Unit) information is non-volatile storage for serial number, part number, asset tag and other inventory information for the baseboard and chassis. The FRU implementation on SE7520JR2 includes write support for OEM-specific records.
- Autonomous Event Logging. The management controller autonomously polls baseboard sensors and generates IPMI Platform Events, also called Event Messages, when an event condition is detected. The events are automatically logged to the System Event Log (SEL).
- System Event Log (SEL). Non-volatile storage for platform health events. Events can be autonomously logged by the BMC, or by sending Event Messages via the system interface or IPMB to the BMC. This enables BIOS, software, and add-in cards to also log events.
- Sensor Data Record (SDR) Repository. Non-volatile storage holding records describing the number and type of management sensors on the baseboard and in the chassis. Includes write support for OEM-specific records and sensors.
- SDR/SEL Timestamp Clock. A clock internally maintained by the management controller that is used for time-stamping events and recording when SDR and SEL contents have changed.
- Intelligent Platform Management Bus (IPMB). The IPMB is a two-wire, multi-master serial bus that provides a point for extending the baseboard management to include chassis management features, and for enabling add-in cards to access the baseboard management subsystem. (Professional and Advanced systems only.)
- Watchdog Timer with selectable timeout actions (power off, power cycle, reset, or NMI) and automatic logging of timeout event
- Direct Platform Control (DPC) LAN Remote Management Connection
- LAN Alerting via PET (Platform Event Trap) format SNMP trap
- Serial/Modem Remote Management Connection (Professional and Advanced systems only)
- Serial/Modem Event Paging/Alerting (Professional and Advanced systems only)

- Platform Event Filtering (PEF)
- Keyboard Controller Style (KCS) IPMI-System Interface (Professional and Advanced systems only)
- SMBus IPMI-System Interface (On-board Platform Instrumentation systems only)
- Intelligent Chassis Management Bus (ICMB) support (Professional and Advanced systems only)
- Remote Boot Control
- Local and Remote Power On/Off/Reset Control
- Local and Remote Diagnostic Interrupt (NMI) Control
- Fault-Resilient Booting
- Control Panel LED Control
- Platform Management Interrupt Routing (Professional and Advanced systems only)
- Power Distribution Board (PDB) monitoring (Professional and Advanced systems only)
- Updateable BMC Firmware
- System Management Power Control (including providing Sleep/Wake and power push-button interfaces)
- Platform Event Filtering (PEF)
- Baseboard Fan Speed Control and Failure Monitoring
- Speaker ‘Beep’ Capability (used to indicate conditions such as FRB failure) (Professional and Advanced systems only)
- Baseboard FRU Information interface
- Diagnostic Interrupt (Control Panel NMI) Handling
- SMI/NMI status monitor (Professional and Advanced systems only)
- System interface to the IPMB (via System Interface Ports) (Professional and Advanced systems only)
- System interface to the PCI SMBus (via System Interface Ports) (Professional and Advanced systems only)
- Secure Mode Control - front panel lock/unlock initiation.
- IPMI v2.0 Management Controller Initialization Agent function (Professional and Advanced systems only)
- Emergency Management Port (EMP) Serial/Modem platform management interface (Professional and Advanced systems only)

- Dedicated Network Interface Controller (NIC) and full TCP/IP software stack (Advanced systems only)

5.2 On-Board Platform Management Features and Functionality

The National Semiconductor PC87431M mini-Baseboard Management Controller (mBMC) is an Application Specific Integrated Circuit (ASIC) with a Reduced Instruction Set Computer (RISC)-based processor and many peripheral devices embedded into it. It is targeted for a wide range of remote-controlled platforms, such as servers, workstations, hubs, and printers.

The mBMC 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 following figure illustrates the block diagram of the mBMC, as it is used in a server management system. The external interface blocks to the mBMC are the discrete hardware peripheral device interface modules shown as blocks outside of the mBMC ASIC.

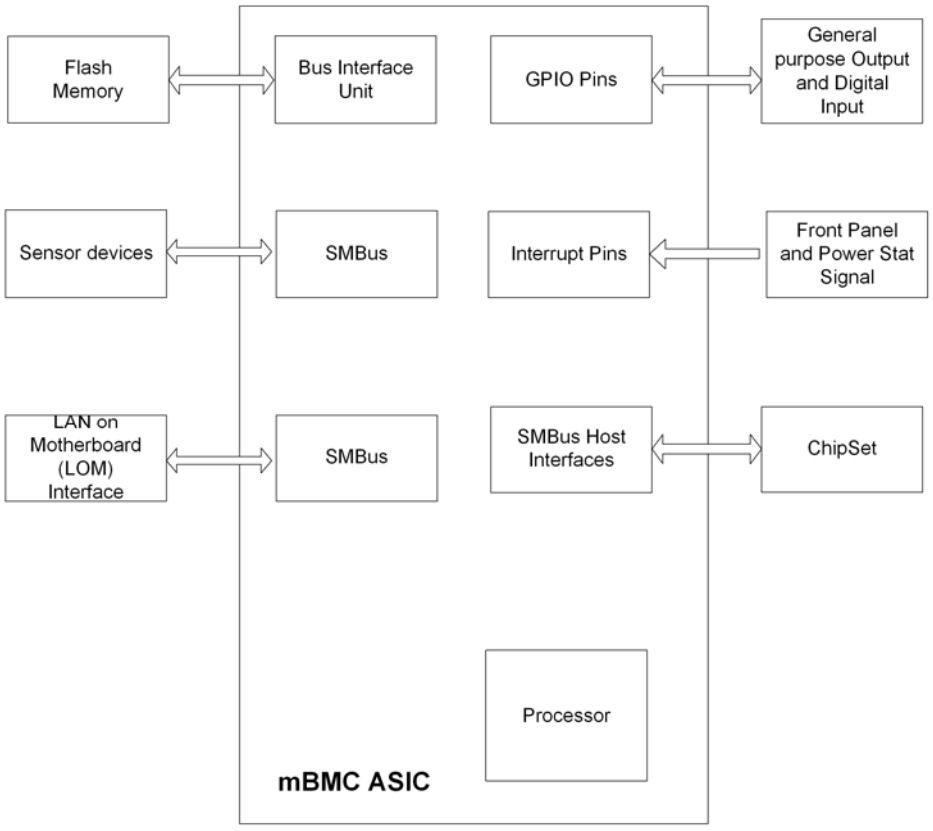


Figure 20. mBMC in a Server Management System

5.2.1 Server Management I²C Buses

The table below describes the server management I²C bus assignments and lists the devices that are connected to the indicated bus. The column labeled "I²C Bus ID" represents the physical I²C bus connected to the mBMC. Only the Peripheral SMBus is available for use with the Write-Read I²C IPMI command.

Table 46: Server Management I²C Bus ID Assignments

I²C Bus ID	Bus Name	Devices Connected
1	Host SMBus	SMBus, PCI slots, ICH5, mBMC, DIMM FRU
2	Peripheral SMBus	SMLink, ICH5, mBMC, SIO 3, LM93, control panel, PDB, Baseboard Temp Sensor, BMC FRU
4	Private Bus 4 – PB4	Network Interface Chipset

5.2.2 Power Control Interfaces

The mBMC is placed between the power button and the chipset so it can implement the Secure Mode feature of disabling the power button, and add additional power control sources to the system. In addition to the mandatory chassis controls, such as power–down and power-up, the mBMC supports power cycle and pulse diagnostic interrupt.

The mBMC C*hassis Control* command supports the following power behavior.

- Power down (0h – C*hassis Control* command): This option asserts a 4s override to the chipset
- Soft Shutdown (5h – C*hassis Control* command): This option generates a 200ms pulse of the chipset power button

5.2.3 External Interface to the mBMC

The following figure shows the data/control flow to and within the functional modules of the mBMC. External interfaces, namely the host system, Lan-On-Motherboard (LOM), and peripherals interact with the mBMC through the corresponding interface modules.

Power supply control functions and control panel control functions are built into the mBMC. The mBMC communicates with the internal modules using its private SMBus. External devices and sensors interact with the mBMC using the peripheral SMBus. LOM communicates through the LOM SMBus.

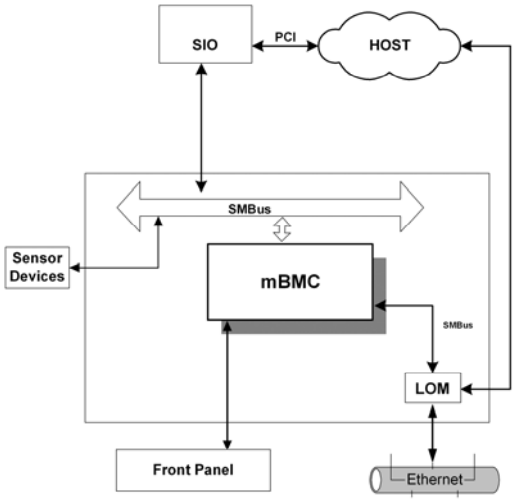


Figure 21. External Interfaces to mBMC

5.3 mBMC Hardware Architecture

The following figure shows an example of the internal functional modules of the mBMC in a block diagram. The mBMC controls various server management functions, such as the system power/reset control, a variety of types of sensor monitoring, system initialization, fault resilient booting (FRB).

The memory subsystem consists of flash memory to hold the mBMC operation code, firmware update code, System Event Log (SEL), Sensor Data Record (SDR) repository, and mBMC persistent data.

A private SMBus provides the mBMC with access to various sensors located in the server system.

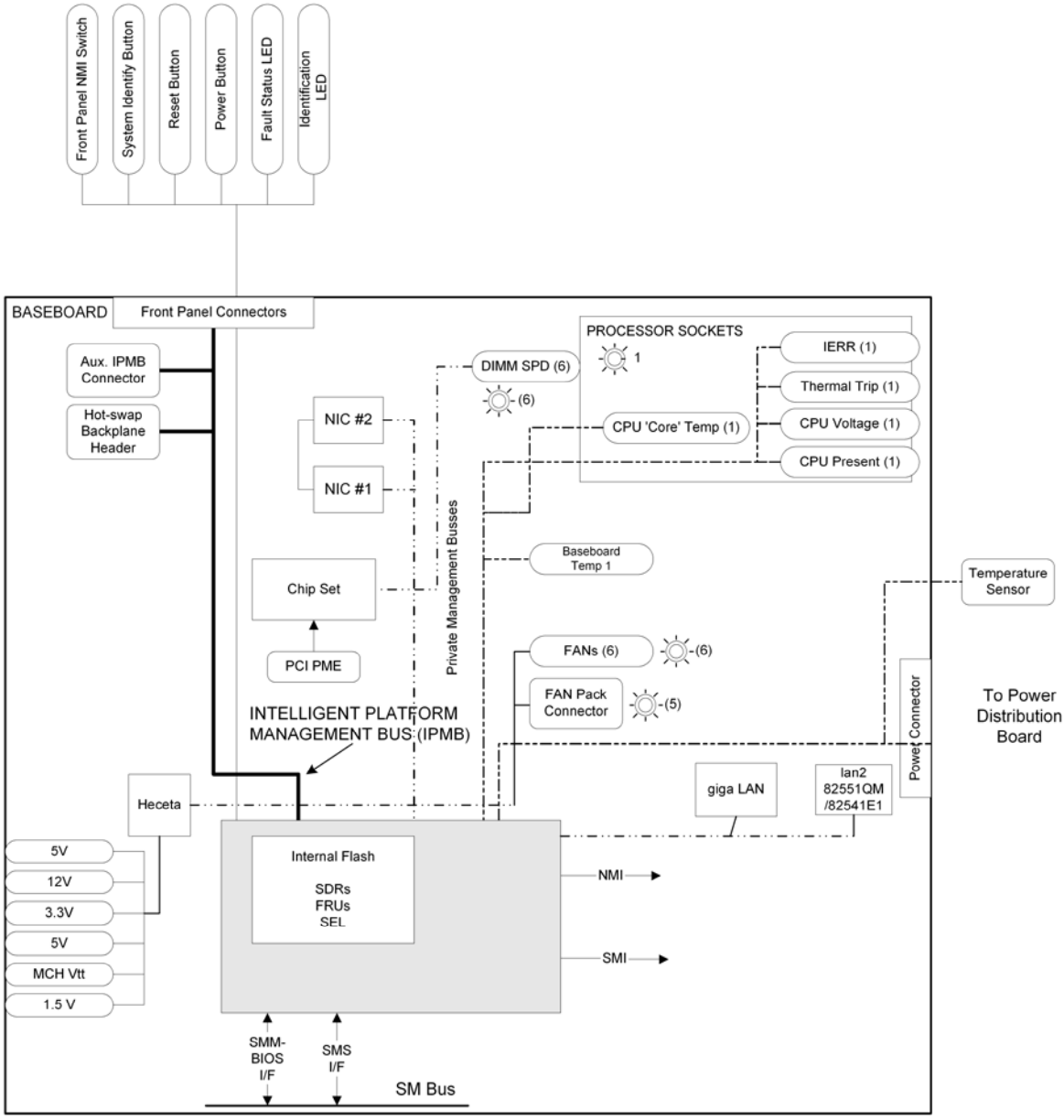


Figure 22. mBMC Block Diagram

5.3.1 Power Supply Interface Signals

The mBMC supports two power supply control signals: *Power On* and *Power Good*. The *Power On* signal connects to the chassis power subsystem through the chipset and is used to request power state changes (asserted = request *Power On*). *Power Good* is a signal from the chassis power subsystem indicating current power state (asserted = power is on).

The following figure shows the power supply control signals and their sources. To turn on the system, the mBMC asserts the *Power On* signal and waits for the *Power Good* signal to assert in response, indicating that DC power is on.

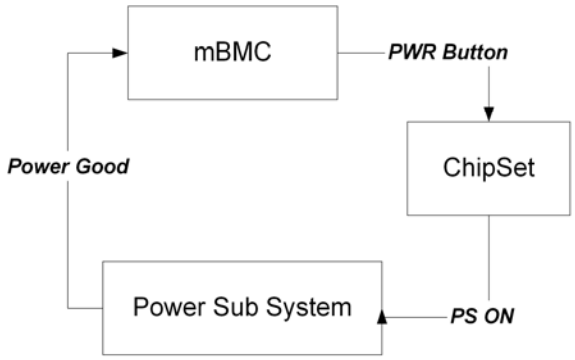


Figure 23. Power Supply Control Signals

The mBMC uses the *Power Good* signal to monitor whether the power supply is on and operational, and to confirm whether the actual system power state matches the intended system on/off power state that was commanded with the *Power On* signal.

De-assertion of the *Power Good* signal generates an interrupt. The mBMC uses this to detect either power subsystem failure or loss of AC power. If AC power is suddenly lost, the mBMC:

1. Immediately asserts a system reset.
2. Powers down the system.
3. Waits for configured system off time, then attempts to power the system back up, depending on system power restore policy.

5.3.2 Power Control Sources

The sources listed in the following table can initiate power-up and/or power-down activity.

Table 47: Power Control Initiators

Source	External Signal Name or Internal Subsystem	Capabilities
Power button	Front control power button	Turns power on or off
mBMC Watchdog Timer	Internal mBMC timer	Turns power off or power cycle
Platform Event Filtering	PEF	Turns power off or power cycle
Command	Routed through command processor	Turns power on or off, or power cycle
Power state retention	Implemented via mBMC internal logic	Turns power on when AC power returns

5.3.3 Power-up Sequence

When turning on the system power after one of the event occurrences, the mBMC executes the following procedure:

1. The mBMC asserts Power Supply (PS) *Power On* via the chipset and waits for the power subsystem to assert *Power Good*. The system is reset.
2. The mBMC initializes all *sensors* to their *Power On* initialization states. The Init Agent is run.
3. The mBMC attempts to boot the system by running the FRB algorithm, if FRB is enabled.

5.3.4 Power-down Sequence

To power down the system, the mBMC effectively performs the sequence of power-up steps in reverse order. It occur as follows:

1. The mBMC asserts system reset.
2. The mBMC de-asserts the *Power On* signal via the chipset.
3. The power subsystem turns off system power upon de-assertion of the *Power On* signal.

5.3.5 System Reset Control

5.3.5.1 Reset Signal Output

The mBMC asserts the *System Reset* signal on the baseboard to perform a system reset. The mBMC asserts the *System Reset* signal before powering the system up. After power is stable as indicated by the power subsystem *Power Good* signal, the mBMC sets the processor enable state as appropriate and de-asserts the *System Reset* signal, taking the system out of reset. The system reset signal responds to the control panel or IPMI commands.

5.3.5.2 Reset Control Sources

The following table shows the reset sources and the actions taken by the system.

Table 48: System Reset Sources and Actions

Reset Source	System Reset?	mBMC Reset
Standby power comes up	No (no DC power)	Yes
DC power comes up	Yes	No
Reset button or in-target probe (ITP) reset	Yes	No
Warm boot (DOS ctrl-alt-del, for example)	Yes	No
Command to reset the system	Yes	No
Set Processor State command	Yes	No
Watchdog timer configured for reset	Yes	No
FRB3 failure	Yes	No
PEF action	Optional	No

5.3.5.3 Control Panel System Reset

The reset button is a momentary contact button on the control panel. Its signal is routed through the control panel connector to the mBMC, which monitors and de-bounces it. The signal must be stable for at least 25 ms before a state change is recognized.

If *Secure Mode* is enabled or the button is forced protected, the reset button does not reset the system. A Platform Security Violation Attempt event message is instead generated.

Control Panel User Interface
When an optional Intel® Management Module is not present, the mBMC acts as the control panel controller[2], processing signals from the control panel switches and LEDs.

When the flexible management connector is populated, the mBMC stops acting on the control panel reset and power button inputs. This becomes the responsibility of the Intel® Management Module.

The mBMC supports three control panel events.

- **Power button assertion**
  A low-level signal at PWBTIN indicates that the power button is being pressed. This input is bridged to the PWBTOUT output if Control Panel Lockout is disabled. The “Control Panel Power Button pressed” event is logged in the SEL.

- **Reset button assertion**
  A low-level signal at RSTIN indicates that the reset button is being pressed. This input is bridged to the RSTOUT output if Control Panel Lockout is disabled. The “Control Panel Reset Button pressed” event is logged in the SEL.

[2] The Intel® Local Control Panel with LCD, is not supported with on-board platform management. Either an IMM Professional Editaion or Advanced Edition must be installed to support this chassis option.

- **Combined power and reset button assertion**
  If DC power is off, an assertion of the PWBTIN while the RSTIN is asserted generates an OEM-specific Control Panel event to PEF. The event attributes are: Sensor Type code - 14h (Button) and Sensor Specific offset - 07h. This PEF action initiates a BIOS CMOS clear request to the system BIOS.

The user interface of the control panel consists of the following indicators:

- Power LED
- Fault/Status LED
- Chassis ID LED

For user input, the standard control panel can provide the following buttons/switches:

- Reset button
- Power button
- NMI/SDI button
- Chassis ID button
- Chassis intrusion switch (optional)

5.3.5.4 Control Panel Indicators

The mBMC is capable of supporting three control panel indicators: Power LED, Fault/Status LED, and Chassis ID LED. The states of these indicators and how they relate to the mBMC/chassis state are detailed below.

5.3.5.4.1 Power LED

The BIOS controls the control panel Power LED as described in the table below.

Table 49: SSI Power LED Operation

State	Power Mode	LED	Description
Power Off	Non-ACPI	OFF	System power is off, and the BIOS has not initialized the chipset.
Power On	Non-ACPI	ON	System power is on, but the BIOS has not yet initialized the chipset.

5.3.5.4.2 Fault / Status LED

The following table shows mapping of sensors/faults to the LED state.

Table 50: Fault / Status LED

Color	Condition	When
Green	Solid	System ready
	Blink	System ready, but degraded: CPU disabled
Amber	Solid	Critical failure: critical fan, voltage, or temperature state
	Blink	Non-critical failure: non-critical fan, voltage, or temperature state
Off	Solid	System not ready: POST error / NMI event / CPU or terminator missing

Critical Condition - Any critical or non-recoverable threshold crossing associated with the following events:

- Temperature, voltage, or fan critical threshold crossing
- Critical Event Logging errors, including System Memory Uncorrectable ECC errors and FSB Bus errors,.

Non-Critical Condition

- Temperature, voltage, or fan non-critical threshold crossing
- Chassis intrusion

Degraded Condition

- One or more processors are disabled by Fault Resilient Boot (FRB)

5.3.5.4.3 Chassis ID LED

The Chassis ID LED provides a visual indication of a system being serviced. The state of the Chassis ID LED is toggled by the chassis ID button or it can be controlled by the *Chassis Identify* command.

Table 51: Chassis ID LED

Color	Condition	When
Blue	Off	Ok
	Blink	Identify button pressed or Chassis Identify command executed

5.3.5.5 Control Panel Inputs

The mBMC monitors the control panel switches and other chassis signals. The control panel input buttons are momentary contact switches, which are de-bounced by the mBMC processor firmware. The de-bounce time is 25 ms.

5.3.5.5.1 Chassis Intrusion

Some platforms support chassis intrusion detection. On those platforms, the mBMC monitors chassis intrusion by polling the server input/output (SIO) device. The state of the chassis intrusion input is provided by the status register of the SIO device. A Chassis Intrusion event is logged in the System Event Log when a change in the input state is detected.

5.3.5.5.2 Power Button

The *Power Button* signal is used to toggle system power. The *Power Button* signal to the mBMC is activated by a momentary contact switch on the control panel assembly.

The mBMC de-bounces the signal. After de-bouncing the signal, the mBMC routes it directly to the chipset via the *Power Button* signal. If the chipset has been initialized by the BIOS, the chipset responds to the assertion of the signal. It reacts to the press of the switch, not the release of it.

If the system is in Secure Mode or if the *Power Button* is forced protected, then when the power switch is pressed, a Platform Security Violation Attempt event message is generated. No power control action is taken.

In the case of simultaneous button presses, the *Power Button* action takes priority over all other buttons. Due to the routing of the de-bounced *Power Button* signal to the chipset, the power signal action overrides the action of the other switch signals.

5.3.5.5.3 Reset Button

An assertion of the control *panel Reset* signal to the mBMC causes the mBMC to start the reset and reboot process. This is immediate and without the cooperation of any software or operating system running on the system.

The reset button is a momentary contact button on the control panel. Its signal is routed through the control panel connector to the mBMC, which monitors and de-bounces it.

If *Secure Mode* is enabled or if the button is forced protected, the reset button does not reset the system, but instead a Platform Security Violation Attempt event message is generated.

5.3.5.5.4 Diagnostic Interrupt Button (Control Panel NMI)

As stated in the *IPMI 1.5 Specification,* a diagnostic interrupt is a non-maskable interrupt or signal for generating diagnostic traces and ‘core dumps’ from the operating system. The mBMC generates NMIs and can be used for an OEM-specific diagnostic control panel interface.

The diagnostic interrupt button is connected to the mBMC through the control panel connector. A diagnostic interrupt button press causes the mBMC to generate a SEL entry that will trigger an NMI PEF OEM action. The event attributes are: Sensor Type code - 13h (Critical Interrupt) and Sensor Specific offset - 0h.

5.3.5.5.5 Chassis Identify Button

The chassis identify button on the control panel toggles the state of the Chassis ID LED. If the Chassis ID LED is off, pressing this button causes the LED to blink for 15 seconds. After this

time, the LED will turn off. If the LED is on, a button press or IPMI *Chassis Identify* command turns off the LED.

Upon assertion of the chassis identify button, a SEL event is generated by the chassis identity sensor button. The event attributes are: Sensor Type code - 14h (Button) and Sensor Specific offset - 1h.

5.3.6 Secure Mode Operation

The mBMC handles the secure mode feature, which allows the control panel power and reset buttons to be protected against unauthorized use or access. Secure mode is a signal from the keyboard controller and is asserted when the keyboard controller is in a locked state. Power and reset buttons are locked and a security violation event is generated if these buttons are pressed while secure mode is active.

Secure Mode state is cleared whenever the System is powered down, the *Set Chassis Capabilities* command is issued to change the Secure Mode state, or the FP_LOCK signal is de-asserted.

5.3.7 Baseboard Fan Control

Fan control is performed by two pulse width modulator (PWM) outputs on the LM93. The 3-pin CPU fan headers (J5F2, J7F1) are not controlled. These operate at a constant speed. The mBMC initializes the LM93 to control fan speeds based on temperature.

The LM93 controls the actual fan speeds based on temperature measurements according to a built-in table. The table itself is loaded as part of the SDR package according to which system configuration is used. In addition, BIOS passes in certain temperature data to the LM93 during POST.

5.3.8 mBMC Peripheral SMBus

The mBMC implements a single private SMBus called the peripheral SMBus. The mBMC supports master-only mode for this SMBus. External agents must use the mBMC's *Master Write/Read I^2C* command if they require direct communication with a device on this bus.

5.3.9 Watchdog Timer

The mBMC implements a fully IPMI 1.5 compatible watchdog timer. See the IPMI 1.5 specification for details on watchdog timer configuration.

5.3.10 System Event Log (SEL)

The mBMC implements the logical System Event Log (SEL) device as specified in the *Intelligent Platform Management Interface Specification, Version 1.5.* The SEL is accessible via all channels. In this way, the SEL information can be accessed through out-of-band interfaces while the system is down. The mBMC supports a maximum SEL size of 92 entries.

If an Intel® Management Module is installed in the server, the mBMC System Event Log is not accessible and is replaced by the Intel Management Module System Event Log.

5.3.10.1 SEL Erasure

It can take up to one minute to clear a System Event Log based upon other concurrent mBMC operations.

5.3.10.2 Timestamp Clock

The mBMC maintains a four-byte internal timestamp clock used by the SEL and SDR subsystems. This clock is incremented once per second and is read and set using the *Get SEL Time* and *Set SEL Time* commands, respectively. The *Get SDR Time* command can also be used to read the timestamp clock. These commands are specified in the *Intelligent Platform Management Interface Specification, Version 1.5.*

The mBMC SEL timestamp is initialized by the BIOS prior to booting to the operating system using the IPMI command *Set SEL Time*.

After a mBMC reset, the mBMC sets the initial value of the timestamp clock to 0x00000000. It is incremented once per second after that. A SEL event containing a timestamp from 0x00000000 to 0x140000000 has a timestamp value that is relative to mBMC initialization.

During POST, the BIOS tells the mBMC the current real-time clock (RTC) time via the *Set SEL Time* command. The mBMC maintains this time, incrementing it once per second, until the mBMC is reset or until the time is changed via another *Set SEL Time* command.

System Management Software is responsible for keeping the mBMC and system time synchronized.

5.3.11 Sensor Data Record (SDR) Repository

The mBMC includes built-in Sensor Data Records (SDRs) that provide platform management capabilities (sensor types, locations, event generation and access information). The SDR Repository is stored in the non-volatile storage area (flash) of the mBMC. The SDR Repository is accessible via all channels. This way, out-of-band interfaces can be used to access SDR Repository information while the system is down. See Table 25 and Table 26 for additional sensor support.

The mBMC supports 2176 bytes of storage for SDR records The SDR defines the type of sensor, thresholds, hysteresis values and event configuration. The mBMC supports up to six threshold values for threshold-based full sensor records, and up to 15 events for non threshold-based full and compact sensor records. The mBMC supports both low-going and high-going sensor devices.

If an Intel Management Module is installed in the server, the mBMC SDRs are not accessible and are replaced by the Intel Management Module SDRs.

5.3.11.1 Initialization Agent

The mBMC implements the internal sensor initialization agent functionality specified in the *Intelligent Platform Management Interface Specification, Version 1.5.* When the mBMC is initialized, or a system is rebooted, the initialization agent scans the SDR repository and configures the mBMC sensors referenced by the SDRs. This includes setting sensor thresholds, enabling/disabling sensor event message scanning, and enabling/disabling sensor event messages.

5.3.12 Field Replaceable Unit (FRU) Inventory Devices

An enterprise-class system typically has FRU information for each major system board, (processor board, memory board, I/O board, etc.). The FRU data includes information such as serial number, part number, model, and asset tag. This information can be accessed in two ways: through IPMI FRU commands or by using Master Write-Read commands.

The mBMC provides FRU device command access to its own FRU device. The mBMC implements the interface for logical FRU inventory devices as specified in the *Intelligent Platform Management Interface Specification, Version 1.5.* This functionality provides commands used for accessing and managing the FRU inventory information associated with the mBMC (FRU ID 0). These commands can be delivered over the Host and LAN channel interfaces.

5.3.12.1 mBMC FRU Inventory Area Format

The mBMC FRU inventory area format follows the Platform Management FRU Information Storage Definition. See the *Platform Management FRU Information Storage Definition, Version 1.0* for details.

The mBMC provides only low-level access to the FRU inventory area storage. It does not validate or interpret the data that is written. This includes the common header area. Applications cannot relocate or resize any FRU inventory areas.

5.3.13 NMI Generation

The mBMC-generated NMI pulse duration is 200 ms. The following may cause the mBMC to generate an NMI pulse:

- Receiving a C*hassis Control* command issued from one of the command interfaces. Use of this command will not cause an event to be logged in the SEL.
- Detecting that the control panel Diagnostic Interrupt button has been pressed. Use of this command will cause a button event to be logged into the SEL Type code - 13h (Critical Interrupt), Sensor Specific offset – 6Fh
- A PEF table entry matching an event where the filter entry has the NMI action indicated.
- Watchdog timer pre-timeout expiration with NMI pre-timeout action enabled.

Once an NMI has been generated by the mBMC, the mBMC will not generate another until the system has been reset or powered down.

5.3.14 SMI Generation

The mBMC can be configured to generate an SMI due to Watchdog timer pre-timeout expiration with SMI pre-timeout interrupt specified.

5.3.15 Event Message Reception

The mBMC supports externally (e.g., BIOS) generated events via the Platform Event Message command. Events received via this command will be logged to the SEL and processed by PEF.

5.3.16 mBMC Self Test

The mBMC performs various tests as part of its initialization. If a failure is determined (e.g., corrupt mBMC FRU, SDR, or SEL), the mBMC stores the error internally.

5.3.17 Messaging Interfaces

This section describes the supported mBMC communication interfaces:

- Host SMS Interface via SMBus interface
- LAN interface using the LOM SMBus

These specifications are defined in the following subsections.

5.3.17.1 Channel Management

The mBMC supports two channels:

- System interface
- 802.3 LAN

Table 52: Suported Channel Assignments

Channel ID	Media Type	Interface	Supports Sessions
1	802.3 LAN	IPMB 1.0	Multi-sessions
2	System Interface	IPMI-SMBus	Session-less

5.3.17.2 User Model

The mBMC supports one anonymous user (null user name) with a settable password. The IPMI *Set User Password* command is supported.

5.3.17.3 Request/Response Protocol

All of the protocols used in the above mentioned interfaces are Request/Response protocols. A *Request Message* is issued to an intelligent device, to which the device responds with a *Response Message*.

As an example, with respect to the IPMB interface, both Request Messages and Response Messages are transmitted on the bus using SMBus Master Write transfers. In other words, a *Request Message* is issued from an intelligent device acting as an SMBus master, and is received by an intelligent device as an SMBus slave. The corresponding *Response Message* is issued from the responding intelligent device as an SMBus master, and is received by the request originator as an SMBus slave.

5.3.17.4 Host to mBMC Communication Interface

The host communicates with the mBMC via the System Management Bus (SMBus). The interface consists of three signals:

- SMBus clock signal (SCLH)

- SMBus data signal (SDAH)
- Optional SMBus alert signal (SMBAH). The signal notifies the host that the PC87431x has data to provide.

When the system main power is off (PWRGD signal is low), the host interface signals are in TRI-STATE to perform “passive” bus isolation between the mBMC SCLH, SDAH and SMBAH signals and the SMBus controller signals. The passive bus isolation can be disabled by host SMBus isolation control (offset 05h;) to support various system designs.

The mBMC is a slave device on the bus. The host interface is designed to support polled operations. Host applications can optionally handle an SMBus alert interrupt, in case the mBMC is unable to respond immediately to a host request. In this case, “Not Ready” is indicated in one of two ways:

  - The host interface bandwidth is limited by the bus clock and mBMC latency. To meet the device latency, the mBMC slows the bus periodically by extending the SMBus clock low interval (SCLH). It is recommended to have a point-to-point connection between the host and mBMC.

- If the mBMC is in the middle of a LAN or peripheral device communication, or if a response to the host request is not yet ready, the mBMC does not acknowledge the device address (“NACK”). This forces the host software to stop and restart the session. The minimum interval between two sessions should be 500 microseconds.

5.3.17.5 LAN Interface

The IPMI Specification v1.5 defines how IPMI messages, encapsulated in RMCP packet format, can be sent to and from the mBMC. This capability allows a remote console application to access the mBMC and perform the following operations:

- Chassis Control, e.g., get chassis status, reset chassis, power-up chassis, power-down chassis
- Get system sensor status
- Get and set system boot options
- Get Field Replaceable Unit (FRU) information
- Get System Event Log (SEL) entries
- Get Sensor Data Records (SDR)
- Set Platform Event Filtering (PEF)
- Set LAN configurations

In addition, the mBMC supports LAN alerting in the form of SNMP traps that conform to the IPMI Platform Event Trap (PET) format.

Table 53: LAN Channel Capacity

LAN Channel Capability	Options
Number of Sessions	1
Number of Users	1
User	Name NULL (anonymous)
User Password	Configurable

LAN Channel Capability	Options
Privilege Levels	User, Operator, Administrator
Authentication Types	None, Straight Password, MD5
Number of LAN Alert Destinations	1
Address Resolution Protocol (ARP)	Gratuitous ARP

5.3.18 Event Filtering and Alerting

The mBMC implements most of the IPMI 1.5 alerting features. The following features are supported:

- PEF
- Alert over LAN

5.3.18.1 Platform Event Filtering (PEF)

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

- Power-down
- Soft-shutdown (pulse ACPI power button signal)
- Power cycle
- Reset
- Diagnostic Interrupt
- Alert

In addition, the mBMC supports the following OEM actions:

- Fault LED action
- Identification LED action
- Device feedback (Generate specified transaction on peripheral SMBus, or change level of DEIO pins)

The power-down, soft-shutdown, power cycle and reset actions can be delayed by a specified number of 100ms up to the maximum PEF delay defined in the IPMI 1.5 specification.

The mBMC maintains an Event Filter table with 30 entries that are used to select which actions to perform and one fixed/read-only Alert Policy Table entry. No alert strings are supported.

Note: All Fault/Status LED and ID LED behaviors are driven off of PEF. PEF should not be disabled and the default entry configuration should not be modified or else those behaviors will be changed.

Each time the PEF module receives an event message, either externally or internally generated, it compares the event data against the entries in the Event Filter table. The mBMC scans all entries in the table and determines a set of actions to be performed according to the entries that were matched. Actions are then executed in order of priority. If there is a combination of power

down, power cycle, and/or reset actions, the actions are performed according to PEF Action Priorities.

Note: An action that has changed from delayed to non-delayed, or an action whose delay time has been reduced automatically has higher priority. The mBMC can be configured to log PEF actions as SEL events.

Table 54: PEF Action Priorities

Action	Priority	Delayed	Type	Note
Power-Down	1	Yes	PEF Action	
Soft-shutdown	2	Yes	OEM PEF Action	Not executed if a power-down action was also selected
Power cycle	3	Yes	PEF Action	Not executed if a power-down action was also selected
Reset	4	Yes	PEF Action	Not executed if a power-down action was also selected
Diagnostic Interrupt	5	No	PEF Action	Not executed if a power-down action was also selected
PET Alert	6	No	PEF Action	When selected, always occurs immediately after detection of a critical event.
Sensor feedback	7	No	OEM PEF Action	When selected, always occurs immediately after detection of a critical event.
IPMB message event	8	No	OEM PEF Action	When selected, always occurs immediately after detection of a critical event.
Fault LED action	9	No	OEM PEF Action	When selected, always occurs immediately after detection of a critical event, and is stopped after the de-assertion of all critical events that requested LED blinking.
Identification LED action	10	No	OEM PEF Action	When selected, always occurs immediately after detection of a critical event.

5.3.18.2 Alert over LAN

LAN alerts are sent as SNMP traps in ASF formatted Platform Event Traps (PET) to a specified alert destination. The Alert over LAN feature is used to send either PET alerts or directed events to a remote system management application, 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. LAN alerts can be used by PEF to send out alerts to selected destination whenever an event matches an event filter table entry. For more information on LAN alerts, see the *IPMI specifications v1.5*

5.3.19 mBMC Sensor Support

The following tables are for the built-in and the external sensors for the platform. There is a management controller locator record as a built-in SDR besides the given below.

mBMC sensors 01h – 08h are internal sensors to the mBMC and are used for event generation only. These sensors are not for use with the 'Get Sensor Reading' IPMI command and may return an error when read.

Table 55: Platform Sensors for On-Board Platform Instrumentation

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData
Physical Security Violation	01	Physical Security 05h	Sensor Specific 6Fh	LAN Leash Lost	As	LAN Leash Lost	Trig Offset
Platform Security Violation	02	Platform Security Violation Attempt 06h	Sensor Pecific 6Fh	Out-of-band access password violation	As	–	Trig Offset
Power Unit Status	03	Power Unit 09h	Sensor Specific 6Fh	Power On/Off Power cycle AC Lost	As	–	Trig Offset
Button	04h	Button 14h	Sensor Specific 6Fh	Power Button Reset Button	As	–	Trig Offset
Watchdog	05h	Watchdog2 23h	Sensor Specific 6Fh	Timer Expired Hard Reset Power Down Power cycle Timer Interrupt	As	–	Trig Offset
System Boot	06h	System boot Initiated 1Dh	Sensor Specific 6Fh	Initiated by power up Initiated by hard reset Initiated by warm reset	As	–	Trig Offset
System PEF Event	07h	System Event 12h	Sensor Specific 6Fh	PEF Action	As	–	Trig Offset
Platform Allert	08h	Platform Alert 24h	Sensor Specific 6Fh	Platform Event Trap generated	As	–	Trig Offset

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value/Offsets	Event Data	PEF Action	SDR Record Type
Physical Security Violation	0Ah	Physical Security 05h	Sensor Specific 6Fh	General Chassis Intrusion	As & De	General Chassis Intrusion	Trig Offset	X	02
CPU1 12v	0Bh	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
CPU2 12v	0Ch	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
BB +1.5V	0Dh	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
BB +1.8V	0Eh	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
BB +3.3V	0Fh	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
BB +5V	10h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
BB +12V	11h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
BB -12V	12h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
FSB Vtt	13h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
MCH Vtt	14h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
SCSI Core(1.8v)	15h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
STBY +3.3V	16h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
Proc1 VCCP	19h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
Proc2 VCCP	1Ah	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
Tach Fan 1	1Bh	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
Tach Fan 2	1Ch	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
Tach Fan 3	1Dh	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
Tach Fan 4	1Eh	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
Tach Fan 5	1Fh	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value/Offsets	Event Data	PEF Action	SDR Record Type
Tach Fan 6	20h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
Tach Fan 7	21h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
Tach Fan 8	22h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
Tach Fan 9	23h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
Proc1 IERR	24h	Processor 07h	Sensor Specific 6Fh	IERR	As	–	Trig Offset	–	02
Proc2 IERR	25h	Processor 07h	Sensor Specific 6Fh	IERR	As	–	Trig Offset	–	02
Proc1 Thermal trip	26h	Processor 07h	Sensor Specific 6Fh	Thermal Trip	As	–	Trig Offset	Fault LED Action	02
Proc2 Thermal trip	27h	Processor 07h	Sensor Specific 6Fh	Thermal Trip	As	–	Trig Offset	Fault LED Action	02
Proc1 Throttle	28h	Temp 01h	Threshold 01h	[u,l][c,nc]	As & De	Analog	Trig Offset	Fault LED Action	01
Proc2 Throttle	29h	Temp 01h	Threshold 01h	[u,l][c,nc]	As & De	Analog	Trig Offset	Fault LED Action	01
Diagnostic Interrupt Button	2Ah	Critical Interrupt 13h	Sensor Specific 6Fh	FP NMI Button	As	–	Trig Offset	NMI Pulse	02
Chassis Identify Button	2Bh	Button 14h	Generic 03h	Sate Deasserted State Assert	As & De	–	Trig Offset	ID LED Action	02
Proc1 Fan	2Ch	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
Proc2 Fan	2Dh	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
Proc1 Core temp	2Eh	Temp 01h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
Proc2 Core temp	2Fh	Temp 01h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	Fault LED Action	01
CPU Configuration Error	30h	Processor 07h	Generic 03h	State Asserted	As & De	Discrete	R, T	Fault LED Action	02
OEM Type 53h	-	OEM Type 53h	N/A	N/A	N/A	N/A	N/A	N/A	N/A

5.3.20 IMM BMC Sensor Support

The following tables are for the built-in and the external sensors for the platform when either an Intel Management Module Professional or Advanced is installed.

Table 56. Platform Sensors for Intel Management Modules - Professional and Advanced

Sensor Name	Sensor Number	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	Rearm	Standby
Power Unit Status	01h	Power Unit 09h	Sensor Specific 6Fh	Power Off Power Cycle A/C Lost Soft Power Control Fault Power Unit Failure Predictive Failure	As	–	Trig Offset	A	X
Power Unit Redundancy	02h	Power Unit 09h	Generic 0Bh	Redundancy Regained Redundancy lost Redundancy Degraded Non-red:Suff res from redund Non-red:Suff res from insuff res Non-red:Insuff res Redundancy Degraded from full redundancy Redundancy Degraded from non-redundant	As	–	Trig Offset	A	X
Watchdog	03h	Watchdog2 23h	Sensor Specific 6Fh	Timer Expired Hard Reset Power Down Power Cycle Timer Interrupt	As & De	–	Trig Offset	A	X
Platform Security Violation	04h	Platform Security Violation Attempt 06h	Sensor Specific 6Fh	Secure mode violation attempt Out-of-band access password violation	As	–	Trig Offset	A	X
Physical Security Violation	05h	Physical Security 05h	Sensor Specific 6Fh	General Chassis Intrusion LAN Leash Lost	As & De	General Chassis Intrusion LAN Leash Lost	Trig Offset	A	X
POST Error	06h	POST error 0Fh	Sensor Specific 6Fh	POST error	As	–	POST Code	A	–

Sensor Name	Sensor Number	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	Rearm	Standby
Critical Inerrupt Sensor	07h	Critical Interrupt 13h	Sensor Specific 6Fh	Front Panel NMI Bus Error	As & De	–	Trig Offset	A	–
Memory	08h	Memory 0Ch	Sensor Specific 6Fh	Uncorrectable ECC	As	–	Trig Offset	A	–
Event Logging Disabled	09h	Event Logging Disabled 10h	Sensor Specific 6Fh	Correctable Memory Error Logging Disabled Log Area Reset/Cleared	As	–	Trig Offset	A	X
Session Audit	0Ah	Session Audit 2Ah	Sensor Specific 6Fh	Session Activation Session Deactivation	As	–	As defined by IPMI	A	X
BB +1.2V Vtt	10h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
BB+1.2V NIC Core	11h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	X
BB +1.5V	12h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
BB +1.8V SCSI Core	13h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
BB +2.5V Memory Voltage	14h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
BB +3.3V	15h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
BB +3.3V Standby	16h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	X
BB +3.3V AUX	17h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	X
BB +5V	18h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
BB +5V Standby	19h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	X
BB +12V	1Ah	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
BB -12V	1Bh	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
BB Vbat	1Ch	Voltage 02h	Digital Discrete 05h	Limit Not Exceeded Limit Exceeded	As & De	–	R, T	A	X
BB Temp	30h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	X
Front Panel Temp	32h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	X
Drive Backplane Temp	35h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–

Sensor Name	Sensor Number	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	Rearm	Standby
Tach Fan 1	40h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	M	–
Tach Fan 2	41h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	M	–
Tach Fan 3	42h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	M	–
Tach Fan 4	43h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	M	–
Tach Fan 5	44h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	M	–
Tach Fan 6	45h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	M	–
Tach Fan 7	46h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	M	–
Tach Fan 8	47h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	M	–
Tach Fan 9	48h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	M	–
Tach Fan 10	49h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	M	–
Tach Fan 11	4Ah	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	M	–
Digital Fan 1	50h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
Digital Fan 2	51h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
Digital Fan 3	52h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
Digital Fan 4	53h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
Digital Fan 5	54h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
Digital Fan 6	55h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
Digital Fan 7	56h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
Digital Fan 8	57h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
Digital Fan 9	58h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–

Sensor Name	Sensor Number	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	Rearm	Standby
Digital Fan 10	59h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
Digital Fan 11	5Ah	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
LVDS SCSI channel 1 terminator fault	60h	Terminator 1Ch	Digital Discrete 06h	Performance Met or Lags	As	–	Trig Offset	A	–
LVDS SCSI channel 2 terminator fault	61h	Terminator 1Ch	Digital Discrete 06h	Performance Met or Lags	As	–	Trig Offset	A	–
Power Supply Status 1	70h	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–	Trig Offset	A	X
Power Supply Status 2 (SR2400)	71h	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–	Trig Offset	A	X
Power Nozzle Power Supply 1	78h	Current 03h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
Power Nozzle Power Supply 2	79h	Current 03h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
Power Gauge V1 rail (+12v) Power Supply 1	7Ah	Current 03h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
Power Gauge V1 rail (+12v) Power Supply 2	7Bh	Current 03h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
Power Gauge (aggregate power) Power Supply 1	7Ch	Other Units 0Bh	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
Power Gauge (aggregate power) Power Supply 2	7Dh	Other Units 0Bh	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
Processor Missing	80h	Module / Board 15h	Digital Discrete 03h	State Asserted State Deasserted	As	–	Trig Offset	A	–
System ACPI Power State	82h	System ACPI Power State 22h	Sensor Specific 6Fh	S0 / G0 S1 S4 S5 / G2 G3 Mechanical Off	As	–	Trig Offset	A	X

Sensor Name	Sensor Number	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	Rearm	Standby
System Event	83h	System Event 12h	Sensor Specific 6Fh	OEM System Boot Event (Hard Reset) PEF Action	As	–	Trig Offset	A	–
Button	84h	Button 14h	Sensor Specific 6Fh	Power Button Sleep Button Reset Button	As	–	Trig Offset	A	X
SMI Timeout	85h	SMI Timeout F3h	Digital Discrete 03h	State Asserted State Deasserted	As	–	Trig Offset	A	–
Sensor Failure	86h	Sensor Failure F6h	OEM Sensor Specific 73h	I2C device not found I2C device error detected I2C Bus Timeout	As	–	Trig Offset	A	X
NMI Signal State	87h	OEM C0h	Digital Discrete 03h	State Asserted State Deasserted	–	–	–	–	–
SMI Signal State	88h	OEM C0h	Digital Discrete 03h	State Asserted State Deasserted	–	–	–	–	–
DIMM Sparing Redundancy	89h	Availability Status 0Bh	Discrete 0Bh	Fully Redundant Non-red:Suff res from redund Non-red:Suff res from insuff res Non-red:Insuff res	As	–	Trig Offset	A	–
DIMM Sparing Enabled	8Ah	Entity Presence 25h	Sensor Specific 6Fh	Entity Present	As	–	Trig Offset	A	–
Memory Mirroring Redundancy	8Bh	Availability Status 0Bh	Discrete 0Bh	Fully Redundant Non-red:Suff res from redund Non-red:Suff res from insuff res Non-red:Insuff res	As	–	Trig Offset	A	–
Memory Mirroring Enabled	8Ch	Entity Presence 25h	Sensor Specific 6Fh	Entity Present	As	–	Trig Offset	A	–
Processor 1 Status	90h	Processor 07h	Sensor Specific 6Fh	IERR Thermal Trip FRB1, FRB2, FRB3 Config Error Presence Disabled	As & De	–	Trig Offset	M	X

Sensor Name	Sensor Number	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	Rearm	Standby
Processor 2 Status	91h	Processor 07h	Sensor Specific 6Fh	IERR Thermal Trip FRB1, FRB2, FRB3 Config Error Presence Disabled	As & De	–	Trig Offset	M	X
Processor 1 Core Temp	98h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
Processor 2 Core Temp	99h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
Processor 1 12v VRM	B8h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
Processor 2 12v VRM	B9h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
Processor 1 Thermal Control	C0h	Temp 01h	Digital Discrete 07h	Transitioned to Non-Critical from OK	As & De	–	Trig Offset	M	–
Processor 2 Thermal Control	C1h	Temp 01h	Digital Discrete 07h	Transitioned to Non-Critical from OK	As & De	–	Trig Offset	M	–
Processor 1 VRD Over Temp	C8h	Temp 01h	Digital Discrete 07h	Transitioned to Non-Critical from OK	As & De	–	Trig Offset	M	–
Processor 2 VRD Over Temp	C9h	Temp 01h	Digital Discrete 07h	Transitioned to Non-Critical from OK	As & De	–	Trig Offset	M	–
Processor 1 Vcc	D0h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
Processor 2 Vcc	D1h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog	R, T	A	–
CPU Configuration Error	D8h	Processor 07h	Generic 03h	State Asserted	As & De	Discrete	R, T	A	-
DIMM 1	E0h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–	Trig Offset	A	–
DIMM 2	E1h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–	Trig Offset	A	–
DIMM 3	E2h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–	Trig Offset	A	–

Sensor Name	Sensor Number	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	Rearm	Standby
DIMM 4	E3h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–	Trig Offset	A	–
DIMM 5	E4h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–	Trig Offset	A	–
DIMM 6	E5h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–	Trig Offset	A	–

5.4 Wired For Management (WFM)

Wired for Management (WMF) is an industry-wide initiative that increases the overall manageability and reduces the total cost of ownership. WFM allows a server to be managed over a network. The system BIOS supports the SMBIOS to help higher-level instrumentation software meet the WFM requirements. Higher-level software can use the information provided by SMBIOS to instrument the desktop management interface (DMI) that are specified in the WFM specification.

5.5 Vital Product Data (VPD)

Vital Product Data (VDP) is product-specific data used for product and product component identification. It is stored in non-volatile memory and preserved through power cycles. The VPD contains information such as Product Serial Number, Product Model Number, Manufacturer Identification, etc.

The VPD is programmed during manufacturing. A user can update certain user-specific VPD information by using the Flash Update utility. The BIOS uses this data and displays it in SMBIOS structures and in BIOS Setup.

5.6 System Management BIOS (SMBIOS)

The BIOS provides support for the SMBIOS specification to create a standardized interface for manageable attributes that are expected to be supported by DMI-enabled computer systems. The BIOS provides this interface via data structures through which the system attributes are reported. Using SMBIOS, a system administrator can obtain the types, capabilities, operational status, installation date and other information about the system components.

Refer to the SE7520JR2 BIOS EPS for detail describing access methods to the SMBIOS structure tables.

6. Error Reporting and Handling

This section defines how errors are handled. Also discussed is the role of the BIOS in error handling and the interaction between the BIOS, platform hardware, and server management firmware with regard to error handling. In addition, error-logging techniques are described and beep codes and POST messages are defined.

Note: The generic term "BMC" may be used throughout this secton when a feature and/or function being described is common to both the mBMC and the Sahalee BMC. If a described feature or function is unique, the specific management controller will be referenced.

6.1 Fault Resilient Booting (FRB)

Fault Resilient Booting (FRB) is a set of BIOS and BMC algorithms and hardware support that allow a multiprocessor system to boot in case of failure of the bootstrap processor (BSP) under certain conditions. FRB functionality will differ depending on whether standard onboard platform instrumentation is used (mBMC) or whether an Intel Management Module is used.

With on-board platform instrumentation, should a processor failure be detected during POST, the mBMC does not have the ability to disable the failed or failing processor. Therefore the system may or may not continue to boot. A FRB-2 error will be generated to the System Event Log (SEL) and an error will be displayed at POST. FRB2 is a BIOS-based algorithm that uses the mBMC IPMI watchdog timer to protect against BIOS hangs during the POST process

On systems that have an Intel Management Module installed, several different levels of FRB are supported: FRB1, FRB2, FRB3, and OS Watchdog Timer. The FRB algorithms detect BSP failures and take steps to disable that processor and reset the system so another processor will run as the BSP.

6.1.1 FRB1 – BSP Self-Test Failures

The BIOS provides an FRB1 timer. Early in POST, the BIOS checks the Built-in Self Test (BIST) results of the BSP. If the BSP fails BIST, the BIOS requests the Sahalee BMC to disable the BSP. The Sahalee BMC disables the BSP, selects a new BSP and generates a system reset. If there is no alternate processor available, the Sahalee BMC generates a beep code and halts the system. If the Sahalee BMC is not installed, then BIOS can only notify the user that the BIST failed; no processors will be disabled.

The BIST failure is displayed during POST and an error is logged to the SEL.

6.1.2 FRB2 – BSP POST Failures

A second timer (FRB2) is set to several minutes by BIOS and is designed to guarantee that the system completes POST. The FRB2 timer is enabled just before the FRB3 timer is disabled to prevent any "unprotected" window of time. Near the end of POST, the BIOS disables the FRB2 timer. If the system contains more than 1 GB of memory and the user chooses to test every DWORD of memory, the watchdog timer is extended before the extended memory test starts, because the memory test can exceed the timer duration. The BIOS will also disable the watchdog timer before prompting the user for a boot password. If the system hangs during POST, before the BIOS disables the FRB2 timer, the Sahalee BMC generates an asynchronous

system reset (ASR). The Sahalee BMC retains status bits that can be read by the BIOS later in the POST for the purpose of disabling the previously failing processor, logging the appropriate event into the System Event Log (SEL), and displaying an appropriate error message to the user.

Options are provided by the BIOS to control the policy applied to FRB2 failures. By default, an FRB2 failure results in the failing processor being disabled during the next reboot. This policy can be overridden to prevent BSP from ever being disabled due to the FRB2 failure or a policy resulting in disabling the BSP after three consecutive FRB2 failures can be selected. These options may be useful in systems that experience fatal errors during POST that are not indicative of a bad processor. Selection of this policy should be considered an advanced feature and should only be modified by a qualified system administrator. The mBMC does not support the option to disable the BSP.

6.1.3 FRB3 – BSP Reset Failures

The BIOS and firmware provide a feature to guarantee that the system boots, even if one or more processors fail during POST. The Sahalee BMC contains two watchdog timers that can be configured to reset the system upon time-out. The first timer (FRB3) starts counting down whenever the system comes out of hard reset. With no Intel® Management Module, only one watchdog timer is present. If the BSP successfully resets and begins executing, the BIOS disables the FRB-3 timer in the BMC and the system continues executing POST. If the timer expires because of the BSP's failure to fetch or execute BIOS code, the Sahalee BMC resets the system and disables the failed processor. The Sahalee BMC continues to change the bootstrap processor until the BIOS successfully disables the FRB3 timer. The BMC generates beep codes on the system speaker if it fails to find a good processor. It will continue to cycle until it finds a good processor. The process of cycling through all the processors is repeated upon system reset or power cycle. Soft resets do not affect the FRB3 timer. The duration of the FRB3 timer is set by system firmware. The mBMC also supports the algorithm described above, with the exception that it does not disable the processor and it will be logged as an FRB2 failure.

6.1.4 OS Watchdog Timer - Operating System Load Failures

The OS Watchdog Timer feature is designed to allow watchdog timer protection of the operating system load process. This is done in conjunction with an operating system-present device driver or application that will disable the watchdog timer once the operating system has successfully loaded. If the operating system load process fails, the BMC will reset the system.

The BIOS shall disable the OS Watchdog Timer before handing control to the OS loader if it is determined to be booting from removable media or the BIOS cannot determine the media type.

If the BIOS is going to boot to a known hard drive, it will read a user option for the OS Watchdog Timer for HDD Boots. If this is disabled, the BIOS will ensure the watchdog timer is disabled and boot. Otherwise the BIOS will read the enabled time value from the option and set the OS Watchdog timer for that value (5, 10, 15, or 20 minutes) before trying to load the operating system. If the OS Watchdog Timer is enabled, the timer is repurposed as an OS Watchdog timer and is referred to by that title as well. WARNING: The BIOS may incorrectly determine that a removable media is a hard drive if the media emulates a hard drive. In this case, the OS Watchdog timer will not be automatically disabled.

If the BIOS is going to boot to a known PXE-compliant device, then the BIOS reads a user option for OS Watchdog Timer for PXE Boots and either disables the timer or enables the timer with a value read from the option (5, 10, 15, or 20 minutes). If the OS Watchdog Timer is enabled, the timer is repurposed as an OS Watchdog Timer and is referred to by that title as well.

If the OS Watchdog Timer is enabled and if a boot password is enabled, the BIOS will disable the OS Watchdog Timer before prompting the user for a boot password regardless of the OS Watchdog Timer option setting. Also, if the user has chosen to enter BIOS setup, the timer will be disabled regardless of option settings. Otherwise, if the system hangs during POST, before the BIOS disables the timer, the BMC generates an asynchronous system reset (ASR). The BMC retains status bits that can be read by the BIOS later in the POST for the purpose of disabling the previously failing processor, logging the appropriate event into the SEL, and displaying an appropriate error message to the user. If no IMM is present no processors will be disabled. As the timer may be repurposed, the BIOS and BMC will also keep track of which timer expired (early FRB2, late FRB2, or OS Watchdog) and display the appropriate error message to the user.

All of the user options are intended to allow a system administrator to set up a system such that during a normal boot no gap exists during POST that is not covered by the watchdog timer. Options are provided by the BIOS to control the policy applied to OS Watchdog timer failures. By default, an OS Watchdog Timer failure will not cause any action. Other options provided by the BIOS are for the system to reset or power off watchdog timer failure. However, it should be noted that these failures will NOT result in a processor being disabled (as could happen with an FRB2 failure).

6.1.5 AP Failures

In systems configured with an Intel Management Module, the BIOS and Sahalee BMC implement additional safeguards to detect and disable the application processors (AP) in a multiprocessor system. If an AP fails to complete initialization within a certain time, it is assumed to be nonfunctional. If the BIOS detects that an AP has failed BIST or is nonfunctional, it requests the Sahalee BMC to disable that processor. Processors disabled by the Sahalee BMC are not available for use by the BIOS or the operating system. Since the processors are unavailable, they are not listed in any configuration tables including SMBIOS tables.

6.1.6 Treatment of Failed Processors

All the failures (FRB3, FRB2, FRB1, and AP failures), including the failing processor, are recorded into the system event log (SEL). The FRB-3 failure is recorded automatically by the BMC while the FRB2, FRB1, and AP failures are logged to the SEL by the BIOS. In the case of an FRB2 failure, some systems will log additional information into the OEM data byte fields of the SEL entry. This additional data indicates the last POST task that was executed before the FRB2 timer expired. This information may be useful for failure analysis.

The Sahalee BMC maintains failure history for each processor in non-volatile storage. This history is used to store a processor's track record. Once a processor is marked "failed," it remains "failed" until the user forces the system to retest the processor by entering BIOS Setup and selecting the "Processor Retest" option. The BIOS reminds the user about a previous processor failure during each boot cycle until all processors have been retested and successfully pass the FRB tests or AP initialization. If all the processors are bad, the system

does not alter the BSP and attempts to boot from the original BSP. Error messages are displayed on the console, and errors are logged in the event log of a processor failure.

If the user replaces a processor that has been marked bad by the system, the system must be informed about this change by running BIOS Setup and selecting that processor to be retested. If a bad processor is removed from the system, the BMC automatically detects this condition and clears the status flag for that processor during the next boot.

Three states are possible for each processor slot:

- Processor installed (status only, indicates processor has passed BIOS POST).
- Processor failed. The processor may have failed FRB2, FRB3, or BIST, and it has been disabled.
- Processor not installed (status only, indicates the processor slot has no processor in it).

Additional information on the FRB may be found in the Sahalee Baseboard Management Controller EPS.

6.2 Memory Error Handling

The chipset will detect and correct single-bit errors and will detect all double-bit memory errors. The chipset supports 4-bit single device data correction (SDDC) when in dual channel mode.

Both single-bit and double-bit memory errors are reported to baseboard management by the BIOS, which handles SMI events generated by the MCH.

Memory Error Handling can be enabled or disabled in system BIOS Setup.

6.2.1 Memory Error Handling in RAS Mode

The MCH supports two memory RAS modes: Sparing and Mirroring. Enabling of Sparing or Mirroring feature are mutually-exclusive. Use system BIOS Setup to configure memory RAS mode.

The following table shows memory error handling with both a mBMC and Sahalee BMC.

Table 57: Memory Error Handling mBMC vs Sahalee

Memory with RAS mode	Server with mBMC	Server with IMM Sahalee BMC
Sparing mode / Mirroring mode	When Sparing or Mirroring occurs: - BIOS will not report memory RAS configuration to mBMC. - BIOS will light the faulty DIMM LED. DIMMs which go off line during OS runtime will be back online on the next system reboot without user intervention. Sparing and Mirroring states are not sticky across system reset.	When Sparing or Mirroring occurs: - BIOS will report memory RAS configuration to BMC. - BIOS will light the faulty DIMM LED. DIMMs which go off line during OS runtime will not be back online on the next system reboot. Sparing and Mirroring states are sticky across system reset. Setting “Memory Retest” option in BIOS Setup will re-enable off-line DIMMs.

Note: BIOS does not support Memory Data Scrubber Error.

6.2.2 Memory Error Handling in non-RAS Mode

If memory RAS features are not enabled in BIOS Setup, BIOS will apply “10 SBE errors in one hour” implementation. Enabling of this implementation and RAS features are mutually-exclusive and automatically handled by system BIOS.

In non-RAS mode, BIOS maintains a counter for Single Bit ECC (SBE) errors. If ten SBE errors occur within an hour, BIOS will disable SBE detection in the chipset to prevent the System Event Log (SEL) from being filled up, and the OS from being halted.

In non-RAS mode, BIOS will assert a Non-Maskable-Interrupt (NMI) on the first Double Bit ECC (DBE) error.

Table 58: Memory Error Handling in non-RAS mode

Non-RAS mode	Server with mBMC	Server with IMM Sahalee BMC
Single Bit ECC (SBE) errors	SBE error events will not be logged. On the 10th SBE error, BIOS will: - Disable SBE detection in chipset. - Light the faulty DIMM LED.	SBE error events will be logged in SEL. On the 10th SBE error, BIOS will: - Disable SBE detection in chipset. - Light the faulty DIMM LED. - Log a SBE termination record to SEL.
Double Bit ECC (DBE) errors	On the 1st DBE error, BIOS will: - Log DBE record to SEL. - Light the faulty DIMM LED. - Generate NMI.	On the 1st DBE error, BIOS will: - Log DBE record to SEL. - Light the faulty DIMM LED. - Generate NMI.

6.2.3 DIMM Enabling

Setting the “Memory Retest” option to “Enabled” in BIOS Setup will bring all DIMM(s) back on line regardless of current states.

After replacing faulty DIMM(s), the “Memory Retest” option must be set to “Enabled”.
Note: this step is not required if faulty DIMM(s) were not taken off-line.

6.2.4 Single-bit ECC Error Throttling Prevention

The system detects, corrects, and logs correctable errors. As long as these errors occur infrequently, the system should continue to operate without a problem.

Occasionally, correctable errors are caused by a persistent failure of a single component. For example, a broken data line on a DIMM would exhibit repeated errors until replaced. Although these errors are correctable, continual calls to the error logger can throttle the system, preventing any further useful work.

For this reason, the system counts certain types of correctable errors and disables reporting if they occur too frequently. Correction remains enabled but calls to the error handler are disabled. This allows the system to continue running, despite a persistent correctable failure. The BIOS adds an entry to the event log to indicate that logging for that type of error has been disabled. Such an entry indicates a serious hardware problem that must be repaired at the earliest possible time.

The system BIOS implements this feature for two types of errors, correctable memory errors and correctable bus errors. If ten errors occur in a single wall-clock hour, the corresponding error handler disables further reporting of that type of error. A unique counter is used for each type of error; i.e., an overrun of memory errors does not affect bus error reporting.

The BIOS re-enables logging and SMIs the next time the system is rebooted.

6.3 Error Logging

This section defines how errors are handled by the system BIOS. Also discussed is the role of the BIOS in error handling and the interaction between the BIOS, platform hardware, and server management firmware with regard to error handling. In addition, error-logging techniques are described and beep codes for errors are defined.

One of the major requirements of server management is to correctly and consistently handle system errors. System error sources can be categorized as follows:

- PCI bus
- Memory multi-bit errors (single-bit errors are not logged)
- Sensors
- Processor internal errors, bus/address errors, thermal trip errors, temperatures and voltages, and GTL voltage levels
- Errors detected during POST, logged as POST errors

Sensors are managed by the mBMC. The mBMC is capable of receiving event messages from individual sensors and logging system events

6.3.1 SMI Handler

The SMI handler handles and logs system-level events that are not visible to the server management firmware. If SEL error logging is disabled in the BIOS Setup utility, no SMI signals are generated on system errors. If error logging is enabled, the SMI handler preprocesses all system errors, even those that are normally considered to generate an NMI.

The SMI handler sends a command to the BMC to log the event and provides the data to be logged. For example, The BIOS programs the hardware to generate an SMI on a single-bit memory error and logs the location of the failed DIMM in the system event log.

6.3.2 PCI Bus Error

The PCI bus defines two error pins, PERR# and SERR#, for reporting PCI parity errors and system errors, respectively. The BIOS can be instructed to enable or disable reporting the PERR# and SERR# through NMI. Disabling NMI for PERR# and/or SERR# also disables logging of the corresponding event. In the case of PERR#, the PCI bus master has the option to retry the offending transaction, or to report it using SERR#. All other PCI-related errors are reported by SERR#. All the PCI-to-PCI bridges are configured so that they generate a SERR# on the primary interface whenever there is a SERR# on the secondary side, if SERR# has been enabled through Setup. The same is true for PERR#.

6.3.3 Processor Bus Error

If the chipset supports ECC on the processor bus then the BIOS enables the error correction and detection capabilities of the processors by setting appropriate bits in the processor model specific register (MSR) and appropriate bits inside the chipset.

In the case of irrecoverable errors on the host processor bus, proper execution of the asynchronous error handler (usually SMI) cannot be guaranteed and the handler cannot be relied upon to log such conditions. The handler will record the error to the SEL only if the system has not experienced a catastrophic failure that compromises the integrity of the handler.

6.3.4 Memory Bus Error

The hardware is programmed to generate an SMI on single-bit data errors in the memory array if ECC memory is installed. The SMI handler records the error and the DIMM location to the system event log. Double-bit errors in the memory array are mapped to the SMI because the mBMC cannot determine the location of the bad DIMM. The double-bit errors may have corrupted the contents of SMRAM. The SMI handler will log the failing DIMM number to the mBMC if the SMRAM contents are still valid. The ability to isolate the failure down to a single DIMM may not be available on certain platforms, and/or during early POST.

6.3.5 System Limit Error

The BMC monitors system operational limits. It manages the A/D converter, defining voltage and temperature limits as well as fan sensors and chassis intrusion. Any sensor values outside of specified limits are fully handled by the BMC. The BIOS does not generate an SMI to the host processor for these types of system events.

6.3.6 Processor Failure

The BIOS detects any processor BIST failures and logs the event. The failed processor can be identified by the first OEM data byte field in the log. For example, if processor 0 fails, the first OEM data byte will be 0. The BIOS depends upon the BMC to log the watchdog timer reset event.

If an OS device driver is using the watchdog timer to detect software or hardware failures and that timer expires, an Asynchronous Reset (ASR) is generated, which is equivalent to a hard reset. The POST portion of the BIOS can query the BMC for a watchdog reset event as the system reboots, and then log this event in the SEL.

6.3.7 Boot Event

The BIOS downloads the system date and time to the BMC during POST and logs a boot event. This record does not indicate an error, and software that parses the event log should treat it as such.

6.4 Error Messages and Error Codes

The BIOS indicates the current testing phase during POST by writing a hex code to I/O location 80h. If errors are encountered, error messages or codes will either be displayed to the video screen, or if an error has occurred prior to video initialization, errors will be reported through a series of audio beep codes.

6.4.1 POST Error Messages

Table 59: Memory BIOS Messages

Message Displayed	Description

Gate20 Error	The BIOS is unable to properly control the motherboard's Gate A20 function, which controls access of memory over 1 MB. This may indicate a problem with the motherboard.
Multi-Bit ECC Error	This message will only occur on systems using ECC enabled memory modules. ECC memory has the ability to correct single-bit errors that may occur from faulty memory modules. A multiple bit corruption of memory has occurred, and the ECC memory algorithm cannot correct it. This may indicate a defective memory module.
Parity Error	Fatal Memory Parity Error. System halts after displaying this message.

Table 60: Boot BIOS Messages

Message Displayed	Description
Boot Failure ...	This is a generic message indicating the BIOS could not boot from a particular device. This message is usually followed by other information concerning the device.
Invalid Boot Diskette	A diskette was found in the drive, but it is not configured as a bootable diskette.
Drive Not Ready	The BIOS was unable to access the drive because it indicated it was not ready for data transfer. This is often reported by drives when no media is present.
A: Drive Error	The BIOS attempted to configure the A: drive during POST, but was unable to properly configure the device. This may be due to a bad cable or faulty diskette drive.
B: Drive Error	The BIOS attempted to configure the B: drive during POST, but was unable to properly configure the device. This may be due to a bad cable or faulty diskette drive.
Insert BOOT diskette in A:	The BIOS attempted to boot from the A: drive, but could not find a proper boot diskette.
Reboot and Select proper Boot device or Insert Boot Media in selected Boot device	BIOS could not find a bootable device in the system and/or removable media drive does not contain media.
NO ROM BASIC	This message occurs on some systems when no bootable device can be detected.

Table 61: Storage Device BIOS Messages

Message Displayed	Description
Primary Master Hard Disk Error	The IDE/ATAPI device configured as Primary Master could not be properly initialized by the BIOS. This message is typically displayed when the BIOS is trying to

Message Displayed	Description
	detect and configure IDE/ATAPI devices in POST.
Primary Slave Hard Disk Error	The IDE/ATAPI device configured as Primary Slave could not be properly initialized by the BIOS. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
Secondary Master Hard Disk Error	The IDE/ATAPI device configured as Secondary Master could not be properly initialized by the BIOS. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
Secondary Slave Hard Disk Error	The IDE/ATAPI device configured as Secondary Slave could not be properly initialized by the BIOS. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
3rd Master Hard Disk Error	The IDE/ATAPI device configured as Master in the 3rd IDE controller could not be properly initialized by the BIOS. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
3rd Slave Hard Disk Error	The IDE/ATAPI device configured as Slave in the 3rd IDE controller could not be properly initialized by the BIOS. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
4th Master Hard Disk Error	The IDE/ATAPI device configured as Master in the 4th IDE controller could not be properly initialized by the BIOS. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
4th Slave Hard Disk Error	The IDE/ATAPI device configured as Slave in the 4th IDE controller could not be properly initialized by the BIOS. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
5th Master Hard Disk Error	The IDE/ATAPI device configured as Master in the 5th IDE controller could not be properly initialized by the BIOS. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
5th Slave Hard Disk Error	The IDE/ATAPI device configured as Slave in the 5th IDE controller could not be properly initialized by the BIOS. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
6th Master Hard Disk Error	The IDE/ATAPI device configured as Master in the 6th IDE controller could not be properly initialized by the BIOS. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
6th Slave Hard Disk Error	The IDE/ATAPI device configured as Slave in the 6th IDE controller could not be properly initialized by the BIOS. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
Primary Master Drive - ATAPI Incompatible	The IDE/ATAPI device configured as Primary Master failed an ATAPI compatibility test. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
Primary Slave Drive - ATAPI Incompatible	The IDE/ATAPI device configured as Primary Slave failed an ATAPI compatibility test. This message is typically displayed when the BIOS is trying to detect and

Message Displayed	Description
	configure IDE/ATAPI devices in POST.
Secondary Master Drive - ATAPI Incompatible	The IDE/ATAPI device configured as Secondary Master failed an ATAPI compatibility test. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
Secondary Slave Drive - ATAPI Incompatible	The IDE/ATAPI device configured as Secondary Slave failed an ATAPI compatibility test. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
3rd Master Drive - ATAPI Incompatible	The IDE/ATAPI device configured as Master in the 3rd IDE controller failed an ATAPI compatibility test. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
3rd Slave Drive - ATAPI Incompatible	The IDE/ATAPI device configured as Slave in the 3rd IDE controller failed an ATAPI compatibility test. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
4th Master Drive - ATAPI Incompatible	The IDE/ATAPI device configured as Master in the 4th IDE controller failed an ATAPI compatibility test. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
4th Slave Drive - ATAPI Incompatible	The IDE/ATAPI device configured as Slave in the 4th IDE controller failed an ATAPI compatibility test. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
5th Master Drive - ATAPI Incompatible	The IDE/ATAPI device configured as Master in the 5th IDE controller failed an ATAPI compatibility test. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
5th Slave Drive - ATAPI Incompatible	The IDE/ATAPI device configured as Slave in the 5th IDE controller failed an ATAPI compatibility test. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
6th Master Drive - ATAPI Incompatible	The IDE/ATAPI device configured as Master in the 6th IDE controller failed an ATAPI compatibility test. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
6th Slave Drive - ATAPI Incompatible	The IDE/ATAPI device configured as Slave in the 6th IDE controller failed an ATAPI compatibility test. This message is typically displayed when the BIOS is trying to detect and configure IDE/ATAPI devices in POST.
S.M.A.R.T. Capable but Command Failed	The BIOS tried to send a S.M.A.R.T. message to a hard disk, but the command transaction failed. This message can be reported by an ATAPI device using the S.M.A.R.T. error reporting standard. S.M.A.R.T. failure messages may indicate the need to replace the hard disk.
S.M.A.R.T. Command Failed	The BIOS tried to send a S.M.A.R.T. message to a hard disk, but the command transaction failed. This message can be reported by an ATAPI device using the S.M.A.R.T. error reporting standard. S.M.A.R.T. failure messages may indicate the need to replace the hard disk.
S.M.A.R.T. Status BAD, Backup and Replace	A S.M.A.R.T. capable hard disk sends this message when it detects an imminent failure. This message can be reported by an ATAPI device using the S.M.A.R.T. error reporting standard. S.M.A.R.T. failure messages may indicate the need to replace the hard disk.
S.M.A.R.T. Capable and Status BAD	A S.M.A.R.T. capable hard disk sends this message

Message Displayed	Description
	when it detects an imminent failure. This message can be reported by an ATAPI device using the S.M.A.R.T. error reporting standard. S.M.A.R.T. failure messages may indicate the need to replace the hard disk.

Table 62: Virus Related BIOS Messages

Message Displayed	Description
BootSector Write !!	The BIOS has detected software attempting to write to a drive's boot sector. This is flagged as possible virus activity. This message will only be displayed if Virus Detection is enabled in AMIBIOS setup.
VIRUS: Continue (Y/N)?	If the BIOS detects possible virus activity, it will prompt the user. This message will only be displayed if Virus Detection is enabled in AMIBIOS setup.

Table 63: System Configuration BIOS Messages

Message Displayed	Description
DMA-2 Error	Error initializing secondary DMA controller. This is a fatal error, often indication a problem with system hardware.
DMA Controller Error	POST error while trying to initialize the DMA controller. This is a fatal error, often indication a problem with system hardware.
Checking NVRAM..Update Failed	BIOS could not write to the NVRAM block. This message appears when the FLASH part is write-protected or if there is no FLASH part (System uses a PROM or EPROM).
Microcode Error	BIOS could not find or load the CPU Microcode Update to the CPU. This message only applies to INTEL CPUs. The message is most likely to appear when a brand new CPU is installed in a motherboard with an outdated BIOS. In this case, the BIOS must be updated to include the Microcode Update for the new CPU.
NVRAM Checksum Bad, NVRAM Cleared	There was an error in while validating the NVRAM data. This causes POST to clear the NVRAM data.
Resource Conflict	More than one system device is trying to use the same non-shareable resources (Memory or I/O).
NVRAM Ignored	The NVRAM data used to store Plug'n'Play (PnP) data was not used for system configuration in POST.
NVRAM Bad	The NVRAM data used to store Plug'n'Play (PnP) data was not used for system configuration in POST due to a data error.
Static Resource Conflict	Two or more Static Devices are trying to use the same resource space (usually Memory or I/O).
PCI I/O conflict	A PCI adapter generated an I/O resource conflict when configured by BIOS POST.
PCI ROM conflict	A PCI adapter generated an I/O resource conflict when configured by BIOS POST.
PCI IRQ conflict	A PCI adapter generated an I/O resource conflict when configured by BIOS POST.
PCI IRQ routing table error	BIOS POST (DIM code) found a PCI device in the system but was unable to figure out how to route an IRQ to the device. Usually this error is causing by an incomplete description of the PCI Interrupt Routing of the system.
Timer Error	Indicates an error while programming the count register

Message Displayed	Description
	of channel 2 of the 8254 timer. This may indicate a problem with system hardware.
Interrupt Controller-1 error	BIOS POST could not initialize the Master Interrupt Controller. This may indicate a problem with system hardware.
Interrupt Controller-2 error	BIOS POST could not initialize the Slave Interrupt Controller. This may indicate a problem with system hardware.

Table 64: CMOS BIOS Messages

Message Displayed	Description
CMOS Date/Time Not Set	The CMOS Date and/or Time are invalid. This error can be resolved by readjusting the system time in AMIBIOS Setup.
CMOS Battery Low	CMOS Battery is low. This message usually indicates that the CMOS battery needs to be replaced. It could also appear when the user intentionally discharges the CMOS battery.
CMOS Settings Wrong	CMOS settings are invalid. This error can be resolved by using AMIBIOS Setup.
CMOS Checksum Bad	CMOS contents failed the Checksum check. Indicates that the CMOS data has been changed by a program other than the BIOS or that the CMOS is not retaining its data due to malfunction. This error can typically be resolved by using AMIBIOS Setup.

Table 65: Miscellaneous BIOS Messages

Message Displayed	Description
Keyboard Error	Keyboard is not present or the hardware is not responding when the keyboard controller is initialized.
PS2 Keyboard not found	PS2 Keyboard support is enabled in the BIOS setup but the device is not detected.
PS2 Mouse not found	PS2 Mouse support is enabled in the BIOS setup but the device is not detected.
Keyboard/Interface Error	Keyboard Controller failure. This may indicate a problem with system hardware.
Unlock Keyboard	PS2 keyboard is locked. User needs to unlock the keyboard to continue the BIOS POST.
System Halted	The system has been halted. A reset or power cycle is required to reboot the machine. This message appears after a fatal error has been detected.

Table 66: USB BIOS Error Messages

Message Displayed	Description
Warning! Unsupported USB device found and disabled!	This message is displayed when a non-bootable USB device is enumerated and disabled by the BIOS.
Warning! Port 60h/64h emulation is not supported by this USB Host Controller!	This message is displayed to indicate that port 60h/64h emulation mode cannot be enabled for this USB host controller. This condition occurs if USB KBC emulation option is set for non-SMI mode.
Warning! EHCI controller disabled. It requires 64bit data support in the BIOS.	This message is displayed to indicate that EHCI controller is disabled because of incorrect data structure. This condition occur if the USB host controller needs 64-

Message Displayed	Description
	bit data structure while the USB is ported with 32-bit data structure.

Table 67: SMBIOS BIOS Error Messages

Message Displayed	Description
Not enough space in Runtime area!!. SMBIOS data will not be available.	This message is displayed when the size of the SMBIOS data exceeds the available SMBIOS runtime storage size.

6.4.2 POST Error Codes

During POST after the video has been initialized, the BIOS outputs the current boot progress codes on the video screen. Progress codes are 32-bit quantities plus optional data. The 32- bit numbers include class, subclass, and operation information. Class and subclass point to the type of the hardware that is being initialized. Operation represents the specific initialization activity.

Based on the data bit availability to display the progress code, a progress code can be customized to fit the data width. The higher the data bit, higher the granularity of allowable information. Progress codes may be reported by system BIOS or option ROMs.

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

- **Warning:** The message is displayed on screen and the error is logged to the SEL. The system will continue booting with a degraded state.
- **Pause:** The message is displayed on the screen and the boot process is paused until the appropriate input is given to either continue the boot process or take corrective action.
- **Halt:** The message is displayed on the screen, an error is logged to the SEL, and the system cannot boot unless the error is corrected.

The error codes are defined by Intel and whenever possible are backward compatible with error codes used on earlier platforms.

All POST error codes are logged in the System Event Log.

Table 68: Error Codes and Messages

Error Code	Error Message	Response
0000	Timer Error	Pause
0003	CMOS Battery Low	Pause
0004	CMOS Settings Wrong	Pause
0005	CMOS Checksum Bad	Pause
0008	Unlock Keyboard	Halt
0009	PS2 Keyboard not found	Not an error
000A	KBC BAT Test failed	Halt
000B	CMOS memory size different	Pause
000C	RAM R/W test failed	Pause
000E	A: Drive Error	Pause
000F	B: Drive Error	Pause
0010	Floppy Controller Failure	Pause

Error Code	Error Message	Response
0012	CMOS time not set	Pause
0014	PS2 Mouse not found	Not an error
0040	Refresh timer test failed	Halt
0041	Display memory test failed	Pause
0042	CMOS Display Type Wrong	Pause
0043	~<INS> Pressed	Pause
0044	DMA Controller Error	Halt
0045	DMA-1 Error	Halt
0046	DMA-2 Error	Halt
0047	Unknown BIOS error. Error code = 147 (this is really a PMM_MEM_ALLOC_ERR)	Halt
0048	Password check failed	Halt
0049	Unknown BIOS error. Error code = 149 (this is really SEGMENT_REG_ERR)	Halt
004A	Unknown BIOS error. Error code = 14A (this is really ADM_MODULE_ERR)	Pause
004B	Unknown BIOS error. Error code = 14B (this is really LANGUAGE_MODULE_ERR)	Pause
004C	Keyboard/Interface Error	Pause
004D	Primary Master Hard Disk Error	Pause
004E	Primary Slave Hard Disk Error	Pause
004F	Secondary Master Hard Disk Error	Pause
0050	Secondary Slave Hard Disk Error	Pause
0055	Primary Master Drive - ATAPI Incompatible	Pause
0056	Primary Slave Drive - ATAPI Incompatible	Pause
0057	Secondary Master Drive - ATAPI Incompatible	Pause
0058	Secondary Slave Drive - ATAPI Incompatible	Pause
0059	Third Master Device Error	Pause
005B	Fourth Master Device Error	Pause
005D	S.M.A.R.T. Status BAD, Backup and Replace	Pause
005E	Password check failed	Pause
0120	Thermal Trip Failure	Pause
0146	Insufficient Memory to Shadow PCI ROM	Pause
0150	BSP Processor failed BIST	Pause
0160	Processor missing microcode – P0	Pause
0161	Processor missing microcode – P1	Pause
0180	BIOS does not support current stepping – P0	Pause
0181	BIOS does not support current stepping – P1	Pause
0192	L2 cache size mismatch	Pause
0193	CPUID, Processor stepping are different	Pause
0194	CPUID, Processor family are different	Pause
0195	Front side bus mismatch.	Pause
0196	CPUID, Processor Model are different	Pause
0197	Processor speeds mismatched	Pause
5120	CMOS Cleared By Jumper	Pause
5121	Password cleared by jumper	Pause
5122	CMOS Cleared By BMC Request	Pause
8104	Warning! Port 60h/64h emulation is not supported by this USB Host Controller !!!	Warning
8105	Warning! EHCI controller disabled. It requires 64bit data support in the BIOS.	Warning
8110	Processor 01 Internal error (IERR)	Warning
8111	Processor 02 Internal error (IERR)	Warning
8120	Processor 01 Thermal Trip error	Warning
8121	Processor 02 Thermal Trip error	Warning

Error Code	Error Message	Response
8130	Processor 01 disabled	Warning
8131	Processor 02 disabled	Warning
8140	Processor 01 failed FRB-3 timer	Warning
8141	Processor 02 failed FRB-3 timer	Warning
8150	Processor 01 failed initialization on last boot.	Warning
8151	Processor 02 failed initialization on last boot.	Warning
8160	Processor 01 unable to apply BIOS update	Pause
8161	Processor 02 unable to apply BIOS update	Pause
8170	Processor 01 failed BIST	Pause
8171	Processor 02 failed BIST	Pause
8180	BIOS does not support current stepping for Processor 1	Pause
8181	BIOS does not support current stepping for Processor 2	Pause
8190	Watchdog timer failed on last boot	Warning
8198	OS boot watchdog timer failure	Pause
8300	BaseBoard Management Controller failed Self Test	Pause
8301	Not enough space in Runtime area!!. SMBIOS data will not be available.	Pause
8305	Primary Hot swap Controller failed to function	Pause
84F1	BIST failed for all available processors	Halt
84F2	BaseBoard Management Controller failed to respond	Pause
84F3	BaseBoard Management Controller in Update Mode	Pause
84F4	Sensor Data Record Empty	Pause
84FF	System Event Log Full	Warning
8500	Bad or missing memory in slot 3A	Pause
8501	Bad or missing memory in slot 2A	Pause
8502	Bad or missing memory in slot 1A	Pause
8504	Bad or missing memory in slot 3B	Pause
8505	Bad or missing memory in slot 2B	Pause
8506	Bad or missing memory in slot 1B	Pause
8600	Primary & Secondary BIOS ID's don't match.	Pause
8601	Override Jumper is set to force boot from lower bank of flash ROM.	Pause
8602	WatchDog Timer Expired(Secondary BIOS maybe bad!).	Pause
8603	Secondary BIOS CheckSum fail.	Pause

The following table indicates error codes that are sent to the Management Module for error logging as a BMC pass-through command. All commands are of “Error” type. The syntax of error logging with the management module and SEL is different. The same error is logged differently in the SEL than with the Management Module.

Table 69: Error Codes Sent to the Management Module

Error code	Error messages
161	Bad CMOS Battery
301	Keyboard failure
102	System Board failure (Timer tick 2 test failure)
106	Diskette Controller Failure
604	Diskette Drive ? failure
163	Time of the day not set
01298000	The BIOS does not support the current stepping of Processor P0
01298001	The BIOS does not support the current stepping of Processor P1

Error code	Error messages
196	Processor cache mismatch detected.
198	Processor speed mismatch detected.
00019700	Processor P0 failed BIST.
00019701	Processor P1 failed BIST.
00150100	Multi-bit error occurred: forcing NMI DIMM = ??
00150100	Multi-bit error occurred: forcing NMI DIMM = ?? DIMM = ?? (could not isolate)
289	DIMM D?? is Disabled.
00150900	SERR/PERR Detected on PCI bus (no source found)
00151100	MCA: Recoverable Error Detected Proc = ??
00151200	MCA: Unrecoverable Error Detected Proc = ??
00151300	MCA: Excessive Recoverable Errors Proc = ??
00151350	Processor MachineCheck Data a Bank = ?? APIC ID = ?? CR4 = ???? ????
00151351	Processor MachineCheck Data b Address = ???? ???? ???? ???? Time Stamp = ???? ???? ???? ????
00151352	Processor MachineCheck Data b Status = ???? ???? ???? ????
00151500	Excessive Single Bit Errors Detected
00151720	Parity Error Detected on Processor bus
00151730	IMB Parity/CRC Error
00151700	Started Hot Spare memory Copy. Failed row/rows = ?? and ?? copied to spare row/rows = ?? and ?? (used on CMIC–HE box)
00151710	Completed Hot Spare memory Copy. Failed row/rows = ?? and ?? copied to spare row/rows = ?? and ?? (used on CMIC–HE box)

6.4.3 BIOS Generated POST Error Beep Codes

The following table lists POST error beep codes. Prior to system video initialization, the BIOS uses these beep codes to communicate error conditions.

Table 70: BIOS Generated Beep Codes

Number of Beeps	Description
1	Memory refresh timer error
2	Parity error in base memory (first 64KB block)
3	Base memory read / write test error
4	Motherboard timer not operational
5	Processor error
6	8042 Gate A20 test error (cannot switch to protected mode)
7	General exception error (processor exception error)
8	Display memory error (system video adapter)
9	ROM checksum error
10	CMOS shutdown register read/write error
11	Cache memory test failed

Table 71: Troubleshooting BIOS Beep Codes

Number of Beeps	Troubleshooting Action
1, 2 or 3	Reseat the memory, or replace with known good modules.
4-7, 9-11	Fatal error indicating a serious problem with the system. Consult your system manufacturer. Before declaring the motherboard beyond all hope, eliminate the possibility of interference by a malfunctioning add-in card. Remove all expansion cards except the video adapter. If the beep codes are generated even when all other expansion cards are absent, the motherboard has a serious problem. Consult your system manufacturer. If the beep codes are not generated when all other expansion cards are absent, one of the add-in cards is causing the malfunction. Insert the cards back into the system one at a time until the problem happens again. This will reveal the malfunctioning add-in card.
8	If the system video adapter is an add-in card, replace or reseat the video adapter. If the video adapter is an integrated part of the system board, the board may be faulty.

6.4.4 Boot Block Error Beep Codes

The following table defines beep codes that may occur if a failure occurs while performing a BIOS Boot Block Update.

Table 72: Boot Block Error Beep Codes

Number of Beeps	Description
1	Insert diskette in floppy drive A:
2	'AMIBOOT.ROM' file not found in root directory of diskette in A:
3	Base Memory error
4	Flash Programming successful
5	Floppy read error
6	Keyboard controller BAT command failed
7	No Flash EPROM detected
8	Floppy controller failure
9	Boot Block BIOS checksum error
10	Flash Erase error
11	Flash Program error
12	'AMIBOOT.ROM' file size error
13	BIOS ROM image mismatch (file layout does not match image present in flash device)
1 long beep	Insert diskette with AMIBOOT.001 File for Multi-Disk Recovery

6.4.5 BMC Generated Beep Codes (Professional/Advanced only)

The Sahalee BMC generates beep codes upon detection of the failure conditions listed in the following table. Each digit in the code is represented by a sequence of beeps whose count is equal to the digit.

Table 73: BMC Beep Code

Code	Reason for Beep
1	Front panel CMOS clear initiated
1-5-1-1	FRB failure (processor failure)
1-5-2-1	No processors installed or processor socket 1 is empty.
1-5-2-3	Processor configuration error (e.g., mismatched VIDs, Processor slot 1 is empty)
1-5-2-4	Front-side bus select configuration error (e.g., mismatched BSELs)
1-5-4-2	Power fault: DC power unexpectedly lost (e.g. power good from the power supply was deasserted)
1-5-4-3	Chipset control failure
1-5-4-4	Power control failure (e.g., power good from the power supply did not respond to power request)

6.5 Checkpoints

6.5.1 System ROM BIOS POST Task Test Point (Port 80h Code)

The BIOS sends a 1-byte hex code to port 80 before each task. The port 80 codes provide a troubleshooting method in the event of a system hang during POST. Table 75 provides a list of the Port 80 codes and the corresponding task description.

6.5.2 Diagnostic LEDs

All port 80 codes are displayed using the Diagnostic LEDs found on the back edge of the baseboard. The diagnostic LED feature consists of a hardware decoder and four dual color LEDs. During POST, the LEDs will display all normal POST codes representing the progress of the BIOS POST. Each code will be represented by a combination of colors from the four LEDs.

The LEDs are capable of displaying three colors: Green, Red, and Amber. The POST codes are divided into two nibbles, an upper nibble and a lower nibble. Each bit in the upper nibble is represented by a Red LED and each bit in the lower nibble is represented by a green LED. If both bits are set in the upper and lower nibbles then both Red and Green LEDs are lit, resulting in an Amber color. If both bits are clear, then the LED is off.

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

- Red bits = 1010b = Ah
- Green bits = 1100b = Ch

Since the red bits correspond to the upper nibble and the green bits correspond to the lower nibble, the two are concatenated to be ACh.

Table 74: POST Progress Code LED Example

LEDs	Red	Green	Red	Green	Red	Green	Red	Green
Ach	1	1	0	1	1	0	0	0

Result	Amber	Green	Red	Off
	MSB			LSB

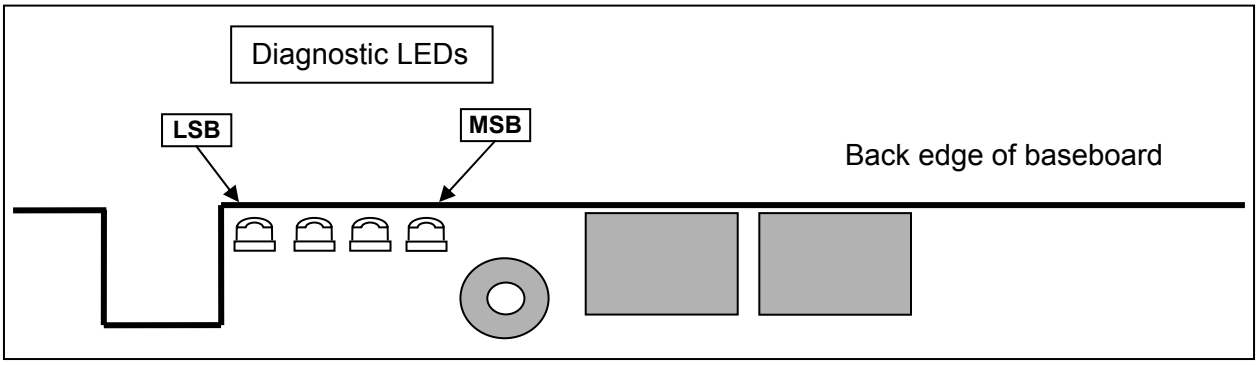


Figure 24. Location of Diagnostic LEDs on Baseboard

6.5.3 POST Code Checkpoints

Table 75: POST Code Checkpoints

Checkpoint	Diagnostic LED Decoder G=Green, R=Red, A=Amber				Description
	MSB			LSB	
03	OFF	OFF	G	G	Disable NMI, parity, video for EGA, and DMA controllers. Initialize BIOS, POST, Run-time data area. Initialize BIOS modules on POST entry and GPNV area. Initialized CMOS as mentioned in the Kernel Variable "wCMOSFlags."
04	OFF	G	OFF	OFF	Check CMOS diagnostic byte to determine if battery power is OK and CMOS checksum is OK. Verify CMOS checksum manually by reading storage area. If the CMOS checksum is bad, update CMOS with power-on default values and clear passwords. Initialize status register A. Initializes data variables that are based on CMOS setup questions. Initializes both the 8259 compatible PICs in the system
05	OFF	G	OFF	G	Initializes the interrupt controlling hardware (generally PIC) and interrupt vector table.
06	OFF	G	G	OFF	Do R/W test to CH-2 count reg. Initialize CH-0 as system timer. Install the POSTINT1Ch handler. Enable IRQ-0 in PIC for system timer interrupt. Traps INT1Ch vector to "POSTINT1ChHandlerBlock."
08	G	OFF	OFF	OFF	Initializes the CPU. The BAT test is being done on KBC. Program the keyboard controller command byte is being done after Auto detection of KB/MS using AMI KB-5.
C0	R	R	OFF	OFF	Early CPU Init Start -- Disable Cache - Init Local APIC
C1	R	R	OFF	G	Set up boot strap processor Information
C2	R	R	G	OFF	Set up boot strap processor for POST
C5	R	A	OFF	G	Enumerate and set up application processors

Checkpoint	Diagnostic LED Decoder				Description
	G=Green, R=Red, A=Amber				
	MSB			LSB	
C6	R	A	G	OFF	Re-enable cache for boot strap processor
C7	R	A	G	G	Early CPU Init Exit
0A	G	OFF	G	OFF	Initializes the 8042 compatible Key Board Controller.
0B	G	OFF	G	G	Detects the presence of PS/2 mouse.
0C	G	G	OFF	OFF	Detects the presence of Keyboard in KBC port.
0E	G	G	G	OFF	Testing and initialization of different Input Devices. Also, update the Kernel Variables. Traps the INT09h vector, so that the POST INT09h handler gets control for IRQ1. Uncompress all available language, BIOS logo, and Silent logo modules.
13	OFF	OFF	G	A	Early POST initialization of chipset registers.
24	OFF	G	R	OFF	Uncompress and initialize any platform specific BIOS modules.
30	OFF	OFF	R	R	Initialize System Management Interrupt.
2A	G	OFF	A	OFF	Initializes different devices through DIM. See DIM Code Checkpoints section of document for more information.
2C	G	G	R	OFF	Initializes different devices. Detects and initializes the video adapter installed in the system that have optional ROMs.
2E	G	G	A	OFF	Initializes all the output devices.
31	OFF	OFF	R	A	Allocate memory for ADM module and uncompress it. Give control to ADM module for initialization. Initialize language and font modules for ADM. Activate ADM module.
33	OFF	OFF	A	A	Initializes the silent boot module. Set the window for displaying text information.
37	OFF	G	A	A	Displaying sign-on message, CPU information, setup key message, and any OEM specific information.
38	G	OFF	R	R	Initializes different devices through DIM. See DIM Code Checkpoints section of document for more information.
39	G	OFF	R	A	Initializes DMAC-1 and DMAC-2.
3A	G	OFF	A	R	Initialize RTC date/time.
3B	G	OFF	R	A	Test for total memory installed in the system. Also, Check for DEL or ESC keys to limit memory test. Display total memory in the system.
3C	G	G	R	R	Mid POST initialization of chipset registers.
40	OFF	R	OFF	OFF	Detect different devices (Parallel ports, serial ports, and coprocessor in CPU, … etc.) successfully installed in the system and update the BDA, EBDA…etc.
50	OFF	R	OFF	R	Programming the memory hole or any kind of implementation that needs an adjustment in system RAM size if needed.
52	OFF	R	G	R	Updates CMOS memory size from memory found in memory test. Allocates memory for Extended BIOS Data Area from base memory.
60	OFF	R	R	OFF	Initializes NUM-LOCK status and programs the KBD typematic rate.
75	OFF	A	R	A	Initialize Int-13 and prepare for IPL detection.
78	G	R	R	R	Initializes IPL devices controlled by BIOS and option ROMs.
7A	G	R	A	R	Initializes remaining option ROMs.
7C	G	A	R	R	Generate and write contents of ESCD in NVRam.
84	R	G	OFF	OFF	Log errors encountered during POST.
85	R	G	OFF	G	Display errors to the user and gets the user response for error.
87	R	G	G	G	Execute BIOS setup if needed / requested.

Checkpoint	Diagnostic LED Decoder G=Green, R=Red, A=Amber				Description
	MSB			LSB	
8C	A	G	OFF	OFF	Late POST initialization of chipset registers.
8D	A	G	OFF	G	Build ACPI tables (if ACPI is supported)
8E	A	G	G	OFF	Program the peripheral parameters. Enable/Disable NMI as selected
90	R	OFF	OFF	R	Late POST initialization of system management interrupt.
A0	R	OFF	R	OFF	Check boot password if installed.
A1	R	OFF	R	G	Clean-up work needed before booting to operating system.
A2	R	OFF	A	OFF	Takes care of runtime image preparation for different BIOS modules. Fill the free area in F000h segment with 0FFh. Initializes the Microsoft IRQ Routing Table. Prepares the runtime language module. Disables the system configuration display if needed.
A4	R	G	R	OFF	Initialize runtime language module.
A7	R	G	A	G	Displays the system configuration screen if enabled. Initialize the CPU's before boot, which includes the programming of the MTRR's.
A8	A	OFF	R	OFF	Prepare CPU for operating system boot including final MTRR values.
A9	A	OFF	R	G	Wait for user input at config display if needed.
AA	A	OFF	A	OFF	Uninstall POST INT1Ch vector and INT09h vector. Deinitializes the ADM module.
AB	A	OFF	A	G	Prepare BBS for Int 19 boot.
AC	A	G	R	OFF	End of POST initialization of chipset registers.
B1	R	OFF	R	A	Save system context for ACPI.
00	OFF	OFF	OFF	OFF	Passes control to OS Loader (typically INT19h).

6.5.4 Bootblock Initialization Code Checkpoints

The Bootblock initialization code sets up the chipset, memory and other components before system memory is available. The following table describes the type of checkpoints that may occur during the bootblock initialization portion of the BIOS:

Table 76: Bootblock Initialization Code Checkpoints

Checkpoint	Diagnostic LED Decoder G=Green, R=Red, A=Amber				Description
	MSB			LSB	
Before D1					Early chipset initialization is done. Early super I/O initialization is done including RTC and keyboard controller. NMI is disabled.
D1	R	R	OFF	A	Perform keyboard controller BAT test. Check if waking up from power management suspend state. Save power-on CPUID value in scratch CMOS.
D0	R	R	OFF	R	Go to flat mode with 4GB limit and GA20 enabled. Verify the bootblock checksum.
D2	R	R	G	R	Disable CACHE before memory detection. Execute full memory sizing module. Verify that flat mode is enabled.
D3	R	R	G	A	If memory sizing module not executed, start memory refresh and do memory sizing in Bootblock code. Do additional chipset initialization. Re-enable CACHE. Verify that flat mode is enabled.

Checkpoint	Diagnostic LED Decoder G=Green, R=Red, A=Amber				Description
	MSB			LSB	
D4	R	A	OFF	R	Test base 512KB memory. Adjust policies and cache first 8MB. Set stack.
D5	R	A	OFF	A	Bootblock code is copied from ROM to lower system memory and control is given to it. BIOS now executes out of RAM.
D6	R	A	G	R	Both key sequence and OEM specific method is checked to determine if BIOS recovery is forced. Main BIOS checksum is tested. If BIOS recovery is necessary, control flows to checkpoint E0. See Bootblock Recovery Code Checkpoints section of document for more information.
D7	R	A	G	A	Restore CPUID value back into register. The Bootblock-Runtime interface module is moved to system memory and control is given to it. Determine whether to execute serial flash.
D8	A	R	OFF	R	The Runtime module is uncompressed into memory. CPUID information is stored in memory.
D9	A	R	OFF	A	Store the Uncompressed pointer for future use in PMM. Copying Main BIOS into memory. Leaves all RAM below 1MB Read-Write including E000 and F000 shadow areas but closing SMRAM.
DA	A	R	G	R	Restore CPUID value back into register. Give control to BIOS POST (ExecutePOSTKernel). See POST Code Checkpoints section of document for more information.

6.5.5 Bootblock Recovery Code Checkpoint

The Bootblock recovery code gets control when the BIOS determines that a BIOS recovery needs to occur because the user has forced the update or the BIOS checksum is corrupt. The following table describes the type of checkpoints that may occur during the Bootblock recovery portion of the BIOS:

Table 77: Bootblock Recovery Code Checkpoint

Checkpoint	Diagnostic LED Decoder G=Green, R=Red, A=Amber				Description
	MSB			LSB	
E0	R	R	R	OFF	Initialize the floppy controller in the super I/O. Some interrupt vectors are initialized. DMA controller is initialized. 8259 interrupt controller is initialized. L1 cache is enabled.
E9	A	R	R	G	Set up floppy controller and data. Attempt to read from floppy. Determine information about root directory of recovery media.
EA	A	R	A	OFF	Enable ATAPI hardware. Attempt to read from ARMD and ATAPI CD-ROM. Determine information about root directory of recovery media.
EB	A	R	A	G	Disable ATAPI hardware. Jump back to checkpoint E9.
EF	A	A	A	G	Read error occurred on media. Jump back to checkpoint EB.
F0	R	R	R	R	Search for pre-defined recovery file name in root directory.
F1	R	R	R	A	Recovery file not found.
F2	R	R	A	R	Start reading FAT table and analyze FAT to find the clusters occupied by the recovery file.
F3	R	R	A	A	Start reading the recovery file cluster by cluster.
F5	R	A	R	A	Disable L1 cache.

Checkpoint	Diagnostic LED Decoder G=Green, R=Red, A=Amber				Description
	MSB			LSB	
FA	A	R	A	R	Check the validity of the recovery file configuration to the current configuration of the flash part.
FB	A	R	A	A	Make flash write enabled through chipset and OEM specific method. Detect proper flash part. Verify that the found flash part size equals the recovery file size.
F4	R	A	R	R	The recovery file size does not equal the found flash part size.
FC	A	A	R	R	Erase the flash part.
FD	A	A	R	A	Program the flash part.
FF	A	A	A	A	The flash has been updated successfully. Make flash write disabled. Disable ATAPI hardware. Restore CPUID value back into register. Give control to F000 ROM at F000:FFF0h.

6.5.6 DIM Code Checkpoints

The Device Initialization Manager (DIM) module gets control at various times during BIOS POST to initialize different Buses. The following table describes the main checkpoints where the DIM module is accessed:

Table 78: DIM Code Checkpoints

Checkpoint	Description
2A	Initialize different buses and perform the following functions: ▪ Reset, Detect, and Disable (function 0). Function 0 disables all device nodes, PCI devices, and PnP ISA cards. It also assigns PCI bus numbers. ▪ Static Device Initialization (function 1). Function 1 initializes all static devices that include manual configured onboard peripherals, memory and I/O decode windows in PCI-PCI bridges, and noncompliant PCI devices. Static resources are also reserved. ▪ Boot Output Device Initialization (function 2). Function 2 searches for and initializes any PnP, PCI, or AGP video devices.
38	Initialize different buses and perform the following functions: ▪ Boot Input Device Initialization (function 3). Function 3 searches for and configures PCI input devices and detects if system has standard keyboard controller. ▪ IPL Device Initialization (function 4). Function 4 searches for and configures all PnP and PCI boot devices. ▪ General Device Initialization (function 5). Function 5 configures all onboard peripherals that are set to an automatic configuration and configures all remaining PnP and PCI devices.

6.5.7 ACPI Runtime Checkpoints

ACPI checkpoints are displayed when an ACPI capable operating system either enters or leaves a sleep state. The following table describes the type of checkpoints that may occur during ACPI sleep or wake events:

Table 79: ACPI Runtime Checkpoints

Checkpoint	Description
AC	First ASL check point. Indicates the system is running in ACPI mode.
AA	System is running in APIC mode.
01, 02, 03, 04, 05	Entering sleep state S1, S2, S3, S4, or S5.
10, 20, 30, 40, 50	Waking from sleep state S1, S2, S3, S4, or S5.

6.5.8 POST Progress FIFO (Professional / Advanced only)

With SE7520JR2 based platforms that utilize either the Professional or Advanced management modules, the Sahalee BMC will maintain a RAM FIFO of the last 16 post progress codes that it has received. Accompanying this FIFO is a timestamp that indicates when the last code was received.

By default, the Sahalee BMC rejects duplicate codes that are received; however, the command interface allows BIOS to explicitly indicate that the code should be stored regardless of whether the previous code was a duplicate.

A corresponding command allows system software to be able to retrieve the contents of the FIFO. This command can be executed via the internal and external interfaces to the Sahallee BMC.
The POST Progress FIFO is volatile. It is cleared whenever the system loses AC power, is powered-down (ACPI S4 or S5), or is reset.

6.5.9 Memory Error Codes

Table 80: Memory Error Codes

Tpoint	Description
001h	MEM_ERR_CHANNEL_B_OFF (DIMM mismatch forced Channel B disabled)
002h	MEM_ERR_CK_PAIR_OFF (Slow DIMM(s) forced clock pair disabled)
0E1h	MEM_ERR_NO_DEVICE (No memory installed)
0E2h	MEM_ERR_TYPE_MISMATCH
0E3h	MEM_ERR_UNSUPPORTED_DIMM (Unsupported DIMM type)
0E4h	MEM_ERR_CHL_MISMATCH

Tpoint	Description
0E5h	MEM_ERR_SIZE_MISMATCH
0E6h	MEM_ERR_ECC_MISMATCH
0E8h	MEM_ERR_ROW_ADDR_BITS
0E9h	MEM_ERR_INTERNAL_BANKS
0EAh	MEM_ERR_TIMING
0EBh	MEM_ERR_INST_ORDER_ERR
0ECh	MEM_ERR_NONREG_MIX
0EDh	MEM_ERR_LATENCY
0EEh	MEM_ERR_NOT_SUPPORTED
0EFh	MEM_ERR_CONFIG_NOT_SUPPORTED
0F0h	SYS_FREQ_ERR (Flag for Unsupported System Bus Freq)
0F1h	DIMM_ERR_CFG_MIX (Usupported DIMM mix)
0F2h	DQS_FAILURE (indicates DQS failure)
0F3h	MEM_ERR_MEM_TEST_FAILURE (Error code for unsuccessful Memory Test)
0F4h	MEM_ERR_ECC_INIT_FAILURE (Error code for unsuccessful ECC and Memory Initialization)

6.6 Light Guided Diagnostics

The baseboard provides system fault/status LEDs in many areas of the board. There are fault LEDs for each DIMM slot and for each processor, and status LEDs for 5-volt stand-by and system state. Operation of some of these LEDs is dependant upon whether an IMM is installed or not. With on-board platform instrumentation, there is limited diagnostic LED support.

- In systems configured with an IMM, the CPU 1 or CPU 2 led is lit to indicate the processor is disabled. DC-Off or AC Cycle will cause the LED to turn off.
- CPU 1 and 2 LEDs are both lit to indicate the baseboard HW has discovered a configuration error. If processor mis-population is detected when using standard on-board platform instrumentation, baseboard hardware will illuminate both processor error LEDs. If an IMM (Professional or Advanced editions) is used, the Sahalee BMC will generate a series of beep codes when this condition is detected and will illuminate the processor 1 fault LED. An AC cycle will cause the LEDs to turn off.
- DIMM fault LEDs are lit by BIOS whenever BIOS disables a specific DIMM.
- The 5-Volt stand-by LED is always lit when 5-volt stand-by is present.
- The Status LED displays the state of the system. It mirrors the state of the Control Panel Status LED. Valid states include: Solid Green, Blinking Green, Blinking Amber, Solid Amber, and Off.

7. Connectors and Jumper Blocks

7.1 Power Connectors

The main power supply connection is obtained using a SSI Compliant 2x12 pin connector. In addition, there are three additional power related connectors; one SSI compliant 2x4 pin power connector (J4J1) providing support for additional 12V, one SSI compliant 1x5 pin connector (J1G1) providing I^2C monitoring of the power supply, and one 1x2 pin IDE power connector (U2E1) providing power to support IDE flash devices. The following tables define their pin-outs

Table 81: Power Connector Pin-out

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

Table 82: 12V Power Connector (J4J1)

Pin	Signal	Color
1	GND	
2	GND	
3	GND	
4	GND	
5	+12Vdc	
6	+12Vdc	
7	+12Vdc	
8	+12Vdc	

Table 83: Power Supply Signal Connector (J1G1)

Pin	Signal	Color
1	5VSB_SCL	Orange
2	5VSB_SDA	Black
3	PS_ALTER_L, Not used	Red
4	3.3V SENSE-	Yellow
5	3.3V SENSE+	Green

Table 84: IDE Power Connector Pinout (U2E1)

Pin	Signal
1	GND
2	5V VCC

7.2 Riser Slots

The baseboard provides two riser slots; one providing PCI-X signals to a riser capable of supporting Low Profile add-in cards, and the other implementing Intel® Adaptive Slot Technology providing both PCI-X and PCI-Express signals to risers capable of supporting full height add-in cards. The following tables show the pin-out for each riser slot.

7.2.1 Low Profile PCI-X Riser Slot

The low profile riser slot pin assignments are shown below. On a given riser card, the PCI add-in slot closest to the baseboard will always have device ID 17. On a three-slot riser card the middle PCI add-in slot will have device ID 18, and the top slot will have device ID 19. The interrupts on the PCI add-in slots should be rotated following the PCI bridge specification 1.0. To prevent anyone from putting a PCI add-in card directly into the riser slot, the connector has been pined out so that Pin 1 is furthest from the board edge. Side B should be closest to the memory DIMMs.

Table 85: Low Profile Riser Slot Pinout

Pin-Side B	PCI Spec Signal	Description	Pin-Side A	PCI Spec Signal	Description
101	-12V		101	RSVD	
100	RSVD		100	+12V	
99	GND		99	RSVD	
98	RSVD		98	+5V	
97	+5V		97	+5V	

Pin-Side B	PCI Spec Signal	Description	Pin-Side A	PCI Spec Signal	Description
96	+5V		96	INTA#	This pin will be connected on the 2U riser to INT_A# of the bottom PCI slot, INT_D# of the middle slot and INT_C# of the top slot.
95	INTB#	This pin will be connected on the 2U riser to INT_B# of the bottom PCI slot, INT_A# of the middle slot and INT_D# of the top slot.	95	INTC#	This pin will be used by 1U/2U riser to bring the INT_C# interrupt on the bottom PCI slot down to the baseboard.
94	INTD#	This pin will be used by 1U/2U riser to bring the INT_D# interrupt on the bottom PCI slot down to the baseboard.	94	+5V	
93	+5V		93	GND	
92	GND		92	REQ3#	Highest PCI Slot (SLOT3)
91	CLK3	Highest PCI Slot (SLOT3)	91	GND	
90	GND		90	GNT3#	Highest PCI Slot (SLOT3)
89	CLK2	Middle PCI Slot (SLOT2)	89	+5V	Was GND
88	GND		88	RSVD	
87	REQ2#	Middle PCI Slot (SLOT2)	87	+5V	Was GND
86	GND		86	LECC4	
85	LECC5		85	GND	Was Vio 3.3V or 1.5V
84	GND		84	LECC3	
83	+3.3V		83	GNT2#	
82	LECC2		82	3.3VAUX	3 slots at 375ma
81	GND		81	RST#	
80	CLK1	Lowest PCI slot (SLOT1)	80	+3.3V	Was VIO 3.3V or 1.5V
79	GND		79	GNT1#	Lowest PCI slot (SLOT1)
78	REQ1#	Lowest PCI slot (SLOT1)	78	GND	
77	+3.3V	Was 3.3V or 1.5V	77	PME#	
76	AD[31]		76	AD[30]	
75	AD[29]		75	+3.3V	
74	GND		74	AD[28]	
73	AD[27]		73	AD[26]	
72	AD[25]		72	GND	
71	+3.3V		71	AD[24]	
70	C/BE[3]#		70	RSVD	Lower slot IDSEL=AD17 Middle Slot=AD18, Top slot=AD19
69	AD[23]		69	+3.3V	
68	GND		68	AD[22]	
67	AD[21]		67	AD[20]	
66	AD[19]		66	GND	
65	+3.3V		65	AD[18]	
64	AD[17]		64	AD[16]	
63	C/BE[2]#		63	+3.3V	

Pin-Side B	PCI Spec Signal	Description	Pin-Side A	PCI Spec Signal	Description
62	GND		62	FRAME#	
61	IRDY#		61	GND	
		KEYWAY			KEYWAY
		KEYWAY			KEYWAY
60	+3.3V		60	TRDY#	
59	DEVSEL#		59	GND	
58	PCI-XCAP		58	STOP#	
57	LOCK#		57	+3.3V	
56	PERR#		56	SMBD	Daisy chain to all slots
55	+3.3V		55	SMBCLK	Daisy chain to all slots
54	SERR#		54	GND	
53	+3.3V		53	PAR /ECC0	
52	C/BE[1]#		52	AD[15]	
51	AD[14]		51	+3.3V	
50	GND		50	AD[13]	
49	AD[12]		49	AD[11]	
47	AD[10]		47	GND	
47	M66EN		47	AD[09]	
46	Mode 2		46	C/BE[0]#	
45	GND		45	+3.3V	Was GND
44	AD[08]		44	+3.3V	
43	AD[07]		43	+3.3V	
42	+3.3V		42	AD[06]	
41	AD[05]		41	AD[04]	
40	AD[03]		40	GND	
39	GND		39	AD[02]	
38	AD[01]		38	AD[00]	
37	+3.3V	Was Vio 3.3V or 1.5V	37	+3.3V	Was Vio 3.3V or 1.5V
36	ACK64# /ECC1		36	REQ64# /ECC6	
35	+5V		35	+5V	
34	+5V		34	+5V	
33	RSVD		33	GND	
32	GND		32	C/BE[7]#	
31	C/BE[6]#		31	C/BE[5]#	
30	C/BE4#		30	V (I/O)	3.3V or 1.5V
29	GND		29	PAR64 /ECC7	
28	AD[63]		28	AD[62]	
27	AD[61]		27	GND	
26	V (I/O)	3.3V or 1.5V	26	AD[60]	
25	AD[59]		25	AD[58]	

Pin-Side B	PCI Spec Signal	Description	Pin-Side A	PCI Spec Signal	Description
24	AD[57]		24	GND	
23	GND		23	AD[56]	
22	AD[55]		22	AD[54]	
21	AD[53]		21	V (I/O)	3.3V or 1.5V
20	GND		20	AD[52]	
19	AD[51]		19	AD[50]	
18	AD[49]		18	GND	
17	V (I/O)	3.3V or 1.5V	17	AD[48]	
16	AD[47]		16	AD[46]	
15	AD[45]		15	GND	
14	GND		14	AD[44]	
13	AD[43]		13	AD[42]	
12	AD[41]		12	V (I/O)	3.3V or 1.5V
		KEYWAY			KEYWAY
		KEYWAY			KEYWAY
11	GND		11	AD[40]	
10	AD[39]		10	AD[38]	
9	AD[37]		9	GND	
8	V (I/O)	3.3V or 1.5V	8	AD[36]	
7	AD[35]		7	AD[34]	
6	AD[33]		6	GND	
5	GND		5	AD[32]	
4			4		
3	PRSNT_N	0=Riser Present	3	GND	
2	GND		2		
1	Size	0=1U, 1= 2U	1	GND	

5V = 12 = 12 or 6 amps 3 slots needs 6 amps for 3 10W boards

3.3V= 19 = 19 or 9.5 amps 3 slots needs 9 amps for 3 10W boards

202 pin connector length = 139.45mm=5.49”

7.2.2 Full Height PCI-X Riser Slot

The full-height/length riser slot is implemented using a 280-pin connector and utilizes Intel Adaptive Slot Technology capable of supporting both PCI-X and PCI-Express riser cards. On a given riser card, the PCI add-in slot closest to the baseboard will always have device ID 17. On a three-slot riser card the middle PCI add-in slot will have device ID 18, and the top slot will have device ID 19. The interrupts on the PCI add-in slots should be rotated following the PCI bridge specification 1.0.

The following table provides the pinout for the Full Height riser slot.

Table 86: Full-height Riser Slot Pinout

Pin-Side B	PCI Spec Signal	Description	Pin-Side A	PCI Spec Signal	Description
140	12V		140	12V	
139	12V		139	12V	
138	Ground		138	GND	
137	-12V		137	3.3VAux	375ma per slot and 3 slots
136	12V		136	Wake#	
135	GND		135	12V	Two slots = 4 amps
134	REFCLK2 +	FL-3GIO Slot 2/PXH - DIF5P	134	3.3V	
133	REFCLK2 +	FL-3GIO Slot 2/PXH - DIF5N	133	PERST_N	
132	GND		132	GND	1 amp per pin
131	GND		131	REFCLK1 +	FL-3GIO Slot 1 – DIF4P
130	HSOp(0)		130	REFCLK1 +	FL-3GIO Slot 1 – DIF4N
129	HSOn(0)		129	GND	
128	GND		128	HSIp(0)	
127	GND		127	HSIn(0)	
126	HSOp(1)		126	GND	
125	HSOn(1)		125	GND	
124	GND		124	HSIp(1)	
123	GND		123	HSIn(1)	
122	HSOp(2)		122	GND	
121	HSOn(2)		121	GND	
120	GND		120	HSIp(2)	
119	GND		119	HSIn(2)	
118	HSOp(3)		118	GND	
117	HSOn(3)		117	GND	
116	GND		116	HSIp(3)	
115	GND		115	HSIn(3)	
114	HSOp(4)		114	GND	
113	HSOn(4)		113	GND	
112	GND		112	HSIp(4)	
111	GND		111	HSIn(4)	
110	HSOp(5)		110	GND	
109	HSOn(6)		109	GND	
108	GND		108	HSIp(5)	
107	GND		107	HSIn(5)	
106	HSOp(6)		106	GND	
105	HSOn(6)		105	GND	
104	GND		104	HSIp(6)	
103	GND		103	HSIn(6)	
102	HSOp(7)		102	GND	

Pin-Side B	PCI Spec Signal	Description	Pin-Side A	PCI Spec Signal	Description
101	HSOn(7)		101	GND	
100	GND		100	HSIp(7)	
99	+5V		99	HSIn(7)	
98	INTB#	This pin will be connected on the 2U riser to INT_B# of the bottom PCI slot, INT_A# of the middle slot and INT_D# of the top slot.	98	GND	
97	INTD#	This pin will be used by 1U/2U riser to bring the INT_B# interrupt from the top and INT_C# from the middle PCI slot down to the baseboard.	97	ZCR_PRSNT_L	From TDI of lowest slot only
96	+5V		96	+5V	
95	Reserved	SLOT_ID_FL, not required as the risers are unique.	95	+5V	
94	+5V		94	ZCR_MSKID_L	From TMS of lowest slot only
93	IOP INTA	SCSI Interrupt A to ZCR. This pin will be used by 1U/2U riser to bring the INT_C# interrupt on the bottom PCI slot down to the baseboard	93	+5V	
92	IOP INTB	SCSI Interrupt B to ZCR. This pin will be used by 1U/2U riser to bring the INT_D# interrupt on the bottom PCI slot down to the baseboard	92	INTA#	This pin will be connected on the 2U riser to INT_A# of the bottom PCI slot, INT_D# of the middle slot and INT_C# of the top slot.
91	GND		91	INTC#	This pin will be used by 1U/2U riser to bring the INT_A# interrupt from the top and INT_B# from the middle PCI slot down to the baseboard.
90	CLK3	Highest PCI Slot (SLOT3)	90	GND	
89	GND		89	REQ3#	Highest PCI Slot (SLOT3)
88	CLK2	Middle PCI Slot (SLOT2)	88	GND	
87	GND		87	GNT3#	Highest PCI Slot (SLOT3)
86	REQ2#	Middle PCI Slot (SLOT2)	86	GND	
85	GND		85	RST#	
84	Reserved		84	GND	
83	GND		83	Reserved	
	KEY			KEY	
	KEY	End of x16 PCI-Express connector		KEY	
82	Reserved		82	+5V	Was Vio 3.3V or 1.5V
81	GND		81	Reserved	
80	CLK1	Lowest PCI slot (SLOT1)	80	GND	
79	Ground		79	GNT2#	Middle PCI Slot (SLOT2)
78	REQ1#	Lowest PCI slot (SLOT1)	78	+3.3V	Was Vio 3.3V or 1.5V

Pin-Side B	PCI Spec Signal	Description	Pin-Side A	PCI Spec Signal	Description
77	+3.3V	Was Vio 3.3V or 1.5V	77	GNT1#	Lowest PCI slot (SLOT1)
76	PME2#	active riser only, PME needed per PCI segment, reserved for passive riser	76	Ground	
75	AD[31]		75	PME1#	for passive slots on both passive and active riser
74	AD[29]		74	PME3#	active riser only, PME needed per PCI segment reserved for passive riser
73	Ground		73	AD[30]	AD[31]
72	AD[27]		72	+3.3V	
71	AD[25]		71	AD[28]	
70	+3.3V		70	AD[26]	
69	C/BE[3]#		69	Ground	
68	AD[23]		68	AD[24]	
67	Ground		67	RSVRD	Reserved
66	AD[21]		66	+3.3V	
65	AD[19]		65	AD[22]	
64	+3.3V		64	AD[20]	
63	AD[17]		63	Ground	
62	C/BE[2]#		62	AD[18]	
61	Ground		61	AD[16]	
60	IRDY#		60	+3.3V	
59	+3.3V		59	FRAME#	
58	DEVSEL#		58	Ground	
57	PCI-XCAP		57	TRDY#	
56	LOCK#		56	Ground	
55	PERR#		55	STOP#	
54	+3.3V		54	+3.3V	
53	SERR#		53	SMBD	Daisy chain to all slots
52	+3.3V		52	SMBCLK	Daisy chain to all slots
51	C/BE[1]#		51	Ground	
50	AD[14]		50	PAR	
49	Ground		49	AD[15]	
48	AD[12]		48	+3.3V	
47	AD[10]		47	AD[13]	
46	M66EN		46	AD[11]	
45	Ground		45	Ground	
44	Ground		44	AD[09]	
43	AD[08]		43	C/BE[0]#	
42	AD[07]		42	+3.3V	
41	+3.3V		41	AD[06]	
40	AD[05]		40	AD[04]	
39	AD[03]		39	Ground	

Pin-Side B	PCI Spec Signal	Description	Pin-Side A	PCI Spec Signal	Description
38	Ground		38	AD[02]	
37	AD[01]		37	AD[00]	
36	+3.3V	Was Vio 3.3V or 1.5V	36	+3.3V	Was Vio 3.3V or 1.5V
35	ACK64#		35	REQ64#	
34	+5V		34	+5V	
33	+5V		33	+5V	
32	Reserved		32	+5V	Was gnd
31	Ground		31	C/BE[7]#	
30	C/BE[6]#		30	C/BE[5]#	
29	C/BE[4]#		29	Ground	Was VIO
28	Ground		28	PAR64	
27	AD[63]		27	AD[62]	
26	AD[61]		26	3.3V	Was GND
25	3.3V		25	AD[60]	
24	AD[59]		24	AD[58]	
23	AD[57]		23	Ground	
22	Ground		22	AD[56]	
21	AD[55]		21	AD[54]	
20	AD[53]		20	3.3V	
19	Ground		19	AD[52]	
18	AD[51]		18	AD[50]	
17	AD[49]		17	Ground	
16	3.3V		16	AD[48]	
15	AD[47]		15	AD[46]	
14	AD[45]		14	Ground	
13	Ground		13	AD[44]	
12	AD[43]		12	AD[42]	
KEY		Reversed PCI-Express	KEY		
KEY		Reversed PCI-Express	KEY		
11	AD[41]		11	3.3V	V
10	Ground		10	AD[40]	
9	AD[39]		9	AD[38]	
8	AD[37]		8	Ground	
7	3.3V		7	AD[36]	
6	AD[35]		6	AD[34]	
5	AD[33]		5	Ground	
4	Ground		4	AD[32]	
3	Type1	Type(1:0) (1U)00 = PCI-Express, (1U)01 = PCI (1U)10 = N/A (1U)11 = N/A	3	PXH_RST_N	Input to reset the PXH on the active Riser
2	Type0	(2U)00=2xPCI-Express+PCI	2	Ground	

Pin-Side B	PCI Spec Signal	Description	Pin-Side A	PCI Spec Signal	Description
		(2U)01=3x PCI (2U)10=PXH 3 PCI-X-D (2U)11=No Riser			
1	Size	0=1U, 1 = 2U	1	PXH_PWR OK	Input to indicate to PXH on active riser that baseboard power is OK

7.3 System Management Headers

The baseboard provides several access points to the management buses built into the baseboard. The following table provides the pinouts for each connector.

7.3.1 Intel® Management Module Connector

A 120-pin connector (J1C1) is included on the baseboard to support the optionally installed “Professional” or “Advanced” Management modules.

Table 87: IMM Connector Pinout (J1C1)

FMC Signal Name	FMC Pin	Description
DVI_TX1M	2	Green TMDS differential DVI output of graphics chip
DVI_TX0M	3	Blue TMDS differential DVI output of graphics chip
DVI_TX1P	4	Green TMDS differential DVI output of graphics chip
DVI_TX0P	5	Blue TMDS differential DVI output of graphics chip
DVI_CLK_TX1CM	8	TMDS differential DVI clock output of graphics chip
DVI_TX2M	9	Red TMDS differential DVI output of graphics chip
DVI_CLK_TX1CP	10	TMDS differential DVI clock output of graphics chip
DVI_TX2P	11	Red TMDS differential DVI output of graphics chip
SIO_MS_DAT	14	KVM mouse data from SIO
SIO_KB_DAT	15	KVM keyboard data from SIO
SIO_MS_CLK	16	KVM mouse clock from SIO
SIO_KB_CLK	17	KVM keyboard clock from SIO
PS2_MS_DAT	18	KVM passthrough mouse data from PS2 connector
PS2_KB_DAT	19	KVM passthrough keyboard data from PS2 connector
PS2_MS_CLK	20	KVM passthrough mouse clock from PS2 connector
PS2_KB_CLK	21	KVM passthrough keyboard clock from PS2 connector
KM_INHIB_N	22	KVM enable of baseboard Switch for mouse and keyboard
FML_SDA	25	Fast Management Link Data In. This signal is driven by the FML Slave, i.e. NIC controller
FML_MCL_I2CSCL	26	Fast Management Link Clock Out. This signal is driven by the FML Master, i.e. FMM. When not configured as FML, this signal is used as I2C clock.

FMC Signal Name	FMC Pin	Description
FML_SINTEX	27	Fast Management Link Slave Interrupt/Clock Extension. This signal is driven by the FML Slave, and has a dual usage: Used as an Alert signal for the slave to notify master that data is ready to be read from slave Used as a clock Extension (Stretching) for the slave to indicate to the master to extend its low period of the clock
FML_MDA_I2CSDA	28	Fast Management Link Data Out. This signal is driven by the FML Master. When not configured as FML, this signal is used as I2C data
ICH_LCLK	31	LPC 33Mhz clock input
USB_M	32	Reserved for future use as USB input. Baseboard can leave as NC
FMM_SYSIRQ	33	KCS interrupt signal from FMM Card.
USB_P	34	Reserved for future use as USB input. Baseboard can leave as NC
ICH_LAD1	35	LPC Address/data bus Bit 1
FMM_RSMRST_N	36	When this signal is asserted, the FMM is held in reset. This is a Standby reset indication, and should be driven by a Standby monitor device such as the Heceta7 or Dallas DS1815
ICH_LFRAME_N	37	LPC Cycle Framing
ICH_LAD0	38	LPC Address/data bus Bit 0
ICH_LAD3	39	LPC Address/data bus Bit 3
ICH_LPCPD_N	40	LPC Power down indication
ICH_LAD2	41	LPC Address/data bus Bit 2
FMM_LPCRST_N	40	LPC bus reset. Must be properly buffered on motherboard to ensure monotonicity
DFP_CLK	46	Serial clock signal for DFP EDID device. Must connect to DFP_CLK pin on the graphics chip.
DFP_DAT	48	Serial data signal for DFP EDID device. Must connect to DFP_DAT pin on the Graphics chip.
IPMB_I2C_5VSB_SDA	49	Connects to IPMB header
IPMB_I2C_5VSB_SCL	50	Connects to IPMB header
SMB_I2C_3VSB_SDA	51	This bus should connect to the PCI slots, ICH, and mBMC (host I/F). An isolated version of this bus (non-Standby) should connect to the DIMMs, and clock buffer(s)
SMB_I2C_3VSB_SCL	52	This bus should connect to the PCI slots, ICH, and mBMC (host I/F). An isolated version of this bus (non-Standby) should connect to the DIMMs, and clock buffer(s)
PERIPH_I2C_3VSB_SDA	53	This bus should connect to the mBMC (Peripheral I/F), SIO, Heceta, Front panel header. A level shifted version of this bus (5V Standby) should connect to the Power Supply header
PERIPH_I2C_3VSB_SCL	54	This bus should connect to the mBMC (Peripheral I/F), SIO, Heceta, Front panel header. A level shifted version of this bus (5V Standby) should connect to the Power Supply header
MCH_I2C_3V_SDA	55	This bus should connect to the Northbridge and I/O bridge (MCH and PXH respectively in the LH chipset). In a system that supports PCI Hot Plug, this bus should also connect to the Power control devices if possible (such as the MIC2591 for PCI-Express for example)
MCH_I2C_3V_SCL	56	This bus should connect to the Northbridge and I/O bridge (MCH and PXH respectively in the LH chipset). In a system that supports PCI Hot Plug, this bus should also connect to the Power control devices if possible (such as the MIC2591 for PCI-Express for example)
LAN_I2C_3VSB_SDA	57	LAN usage

FMC Signal Name	FMC Pin	Description
LAN_I2C_3VSB_SCL	58	LAN usage
HDD_FLT_LED_N	64	Drive Fault LED output driven when FMM detects a bad drive from the Hot Swap controller on the Hot Swap disk Drive sub-system.
FMM_PS_PWR_ON_N	65	Power On Request to the system Power Supply
COOL_FLT_LED_N	66	Cool Fault LED output driven when FMM detects a bad Fan if SSI front panel is detect.
FMM_CPU_VRD_EN	67	This signal is driven by the FMM to enable the CPU VRDs and allow the VRD power good chain to complete. This signal can also be used to keep the system in reset for an extended time, beyond what the chipset RST_BTN_N can provide.
FMM_SCI_N	68	SCI event request. If ACPI EC is supported by FMM, this signal is used for ACPI interrupts.
ICH_PWR_BTN_N	69	FMM pass through of Front panel power button to chipset
FMM_SPKR_N	72	FMM uses this to create Beep Codes on the system audible alarm. This signal is configured as an Open Drain buffer in the FMM and must be pulled up to 3.3V Standby on the motherboard
FP_NMI_BTN_N	73	NMI / Diagnostic interrupt from front panel. Actual NMI generated by SMBUS command to mBMC
FP_SLP_BTN_N	74	Front panel Sleep Button input, if used
FP_ID_BTN_N	75	Front panel ID button, will cause the ID light to toggle
SYS_PWR_GD	76	Signal from the end of the baseboard VRD Power good chain. This signal should be the last VRD power good indication generated on the baseboard. Usually this would be the signal feeding the Chipset Power OK input. Used by FMM in conjunction with RST_PWRGD_PS to determine if all critical VRDs have successfully reached their nominal value.
CPU2_SKTOCC_N	80	Indicates that a Processor is in the application processor socket
CLK_32K_RTC	81	This signal is used for “Synchronized clock with system RTC”. FMM can synchronize own RTC with system RTC. IPMI define synchronized method. clock comes from the Chipset RTC function.
CPU1_SKTOCC_N	82	Indicates that a Processor is in the primary processor socket. If this socket is detected empty and there’s an attempt to power up the system, the FMM will output an Error Beep Code and prevent the System from turning on
FMM_SOUT	85	EMP/SOL Serial Data Out. This is the Serial Port data output from FMM and should be connected to the SIN signal in the SIO3 device
FMM_SIN	86	EMP/SOL Serial Data In. This is the Serial Port data input into the FMM and should be connected to the SOUT signal in the SIO3 device
FMM_DCD_N	87	EMP/SOL Data Carrier Detect. This is the Serial Port Data Carrier Detect input into the FMM and should be connected to the DCD signal in the SIO3 device
FMM_RTS_N	88	EMP/SOL Request to Send. This is the Serial Port Request to Send output from FMM and should be connected to the CTS (Clear to Send) signal in the SIO3 device
FMM_DTR_N	89	EMP/SOL Data Terminal Ready. This is the Serial Port Data Terminal Ready output from FMM and should be connected to the DSR (Data Set Ready) signal in the SIO3 device
FMM_CTS_N	90	EMP/SOL Clear to Send. This is the Serial Port Clear to Send input into the FMM and should be connected to the RTS (Ready to Send) signal in the SIO device
ICMB_RX	93	Inter Chassis Communication Management Bus receive data
ICMB_TX	94	Inter Chassis Communication Management Bus transmit data
ICMB_TX_EN	96	Inter Chassis Communication Management Bus transceiver enable

FMC Signal Name	FMC Pin	Description
FMM_RI_BUF_N	97	Ring Indicator from the EMP serial port on the baseboard
RST_PWRGD_PS	101	Power good signal from power subsystem. In typical system, this signal is connected to PWR_OK signal on power supply. This signal is monitored by the FMM to detect a Power Supply failure
LAN_SMBALERT_N	102	Alert signal from the motherboard NIC (LOM).
ICH_SLP_S4_N	103	Power Off request from the Chipset
ICH_SMI_BUFF_N	105	SMI signal from Chipset. This signal is monitored by the FMM to detect an “SMI Time-out” condition. If this signal is asserted for longer than a predefined SMI Time-out timer, an event is logged and the FMM interrogates the chipset for further data, such as fatal errors.
CHPSET_ERR_ALERT_N	106	When available from chipset, indicates that a error occurred and FMM will need interrogate Chipset for further data, such as fatal errors. If not available, leave as NC.
FP_RST_BTN_N	109	Front panel Reset Button input.
ICH_RST_BTN_N	110	Passthrough of front panel Reset button to the chipset. FMM chassis control command will also use this.
FP_PWR_BTN_N	113	Front panel power button input.
FMM_IRQ_SMI_N	116	FMM might use this signal to generate an SMI to the system.
FMM_PRES_N	120	When FMM is present, this signal is asserted. This signal can be used to notify BIOS that a module is present (via routing to GPIO), as well as to control any logic which behaves differently when FMM is present, such as the FML mux (if supported), etc

7.3.2 ICMB Header

A white 5-pin header (J1D1) located on the left side of the baseboard near the internal SCSI connector cutout.

Table 88: ICMB Header Pin-out (J1D1)

Pin	Signal Name	Type	Description
1	5 V standby	Power	
2	Transmit	Signal	UART signals
3	Transmit Enable	Signal	UART signals
4	Receive	Signal	UART signals
5	Ground	GND	

7.3.3 IPMB Header

When either the “Professional” or “Advanced” management modules are installed, the yellow 3-pin IPMB connector (J3F1) can be used to access the IPMB bus.

Note: There is no IPMB bus available with standard on-board platform instrumentation.

Table 89: IPMB Connector Pin-out (J3F1)

Pin	Signal Name	Description
1	Local I2C SDA	BMC IMB 5 V STNDBY Data Line
2	GND	
3	Local I2C SCL	BMC IMB 5 V STNDBY Clock Line

7.3.4 OEM RMC Connector (J3B2)

A white eight pin connector (J3B2) used for OEM specific management cards.

Table 90: OEM RMC Connector Pinout (J3B2)

Pin	Signal Name	Description
1	PERIPH_I2C_3VSB_SDA	
2	PERIPH_I2C_3VSB_SCL	
3	POST_STATUS	
4	+5V	
5	GROUND	
6	5V_STBY	
7	ICH5_SYS_RST_L	
8	FP_PWR_BTN_RMC	

7.4 Control Panel Connectors

The Server Board SE7520JR2 provides three control panel interconnects: a high density 100-pin connector for use in the Intel Server Chassis SR1400 1U and SR2400 2U with backplane installed, a 50-pin control panel connector used in Intel's chassis with no backplane installed, and a SSI standard 34-pin connector for use in third-party reference chassis. The following tables provide the pinouts for each connector.

Table 91: 100-Pin Flex Cable Connector Pin-out (For Intel Chassis w/Backplane) (J2J1)

Pin	Signal Name	Pin	Signal Name
A1	GND	B1	V_IO_VSYNC_BUFF_FP_L
A2	V_IO_RED_CONN_FP	B2	V_IO_HSYNC_BUFF_FP_L
A3	V_IO_GREEN_CONN_FP	B3	TEMP_PWM_R
A4	V_IO_BLUE_CONN_FP	B4	SPB_DCD_L
A5	VIDEO_IN_USE	B5	SPB_CTS_L
A6	SPB_DTR_L	B6	SPB_SOUT_L
A7	SPB_RTS _L	B7	SPB_EN_L
A8	SPB_SIN	B8	LAN_ACT_B_L
A9	SPB_DSR	B9	LAN_LINKB_R
A10	FP_NMI_BTN_L	B10	FP_CHASSIS_INTRU
A11	GND	B11	PS_I2C_5VSB_SCL
A12	FP_ID_BTN_L	B12	PS_I2C_5VSB_SDA
A13	P5V_STBY	B13	LAN_ACT_A_L
A14	FP_RST_BTN_L	B14	LAN_LINKA_R
A15	HDD_FAULT_LED_L	B15	FP_ID_LED_R
A16	FP_PWR_BTN_L	B16	IPMB_I2C_5VSB_SCL
A17	HDD_LED_ACT_L	B17	P5V_STBY
A18	P3V3	B18	FP_STATUS_LED2_R
A19	IPMB_I2C_5VSB_SDA	B19	FP_STATUS_LED1_R

Pin	Signal Name	Pin	Signal Name
A20	GND	B20	FP_PWR_LED_L
A21	P5V_STBY	B21	RST_IDE_S_L
A22	RST_IDE_L	B22	FD_HDSEL_L
A23	FD_DSKCHG_L	B23	FD_RDATA_L
A24	FD_WPD_L	B24	FD_WDATA_L
A25	FD_TRK0_L	B25	FD_STEP_L
A26	FD_WGATE_L	B26	FD_MTR0_L
A27	FD_DIR_L	B27	FD_DENSEL0
A28	FD_DS0_L	B28	FD_INDEX_L
A29	GND	B29	IDE_SDD_8
A30	IDE_SDD_7	B30	IDE_SDD_9
A31	IDE_SDD_6	B31	IDE_SDD_10
A32	IDE_SDD_5	B32	IDE_SDD_11
A33	IDE_SDD_4	B33	IDE_SDD_12
A34	IDE_SDD_3	B34	IDE_SDD_13
A35	IDE_SDD_2	B35	IDE_SDD_14
A36	IDE_SDD_1	B36	IDE_SDD_15
A37	IDE_SDD_0	B37	IDE_SDDREQ
A38	GND	B38	IDE_SDIOW_L
A39	IDE_SDDACK_L	B39	IDE_SDIOR_L
A40	IDE_SDA_1	B40	IDE_SIORDY
A41	IDE_SDA_0	B41	IRQ_IDE_S
A42	IDE_SDCS1_L	B42	IDE_SDA_2
A43	IDE_SEC_HD_ACT_L	B43	IDE_SDCS3_L
A44	GND	B44	FAN_SPEED_CNTL1
A45	FAN_TACH5	B45	R_FAN_PRESENT
A46	FAN_TACH6	B46	BB_LED_FAN5_R
A47	FAN_TACH7	B47	BB_LED_FAN6_R
A48	FAN_TACH8	B48	BB_LED_FAN7_R
A49	FAN_SPEED_CNTL2	B49	BB_LED_FAN8_R
A50	P5V_STBY	B50	GND

Table 92: 50-Pin Control Panel Connector (Intel Chassis w/No Backplane) (J1J2)

Pin#	Signal Name	Pin #	Signal Name
1	PWR_LCD_5VSB	2	PWR_LCD_5VSB
3	TP_J1H5_3	4	HDD_LED_ACT_L
5	FP_STATUS_LED1_L	6	RST_IDE_L
7	FP_STATUS_LED2_L	8	5VSTBY
9	5VSTBY	10	FP_PWR_LED_L
11	3.3V	12	IPMB_I2C_5VSB_SDA
13	GND	14	IPMB_I2C_5VSB_SCL
15	FP_ID_LED_L	16	FP_PWR_BTN_L
17	LAN_LINKB_L	18	HDD_FAULT_LED_L

Pin#	Signal Name	Pin #	Signal Name
19	LAN_ACT_B_L	20	FP_RST_BTN_L
21	PS_I2C_5VSB_SDA	22	GND
23	PS_I2C_5VSB_SCL	24	FP_ID_BTN_L
25	FP_CHASSIS_INTRU	26	TP_J1H5_26
27	LAN_LINKA_L	28	LAN_ACT_A_L
29	GND	30	FP_NMI_BTN_L
31	SPB_EN_L	32	SPB_DSR
33	SPB_SOUT	34	SPB_SIN
35	SPB_CTS_L	36	SPB_RTS_L
37	SPB_DCD_L	38	SPB:DTR_L
39	TEMP_PWM_R	40	VIDEO_IN_USE
41	GND	42	V_IO_VSYNC_BUFF_FP_L
43	GND	44	V_IO_HSYNC_BUFF_FP_L
45	GND	46	V_IO_BLUE_CONN_FP
47	GND	48	V_IO_GREEN_CONN_FP_L
49	GND	50	V_IO_RED_CONN_FP_L

Table 93: Control Panel SSI Standard 34-Pin Header Pin-out

Pin	Signal Name	Pin	Signal Name
1	P5V	2	P5V_STBY
3	Key	4	P5V_STBY
5	FP_PWR_LED_L	6	FP_COOL_FLT_LED_R
7	P5V	8	P5V_STBY
9	HDD_LED_ACT_R	10	FP_STATUS_LED2_R
11	FP_PWR_BTN_L	12	LAN_ACT_A_L
13	GND	14	LAN_LINKA_L
15	Reset Button	16	PS_I2C_5VSB_SDA
17	GND	18	PS_I2C_5VSB_SCL
19	FP_SLP_BTN_L	20	FP_CHASSIS_INTRU
21	GND	22	LAN_ACT_B_L
23	FP_NMI_BTN_L	24	LAN_LINKB_L
25	Key	26	Key
27	P5V_STBY	28	P5V_STBY
29	FP_ID_LED_L	30	FP_STATUS_LED1_R
31	FP_ID_BTN_L	32	P5V
33	GND	34	FP_HDD_FLT_LED_R

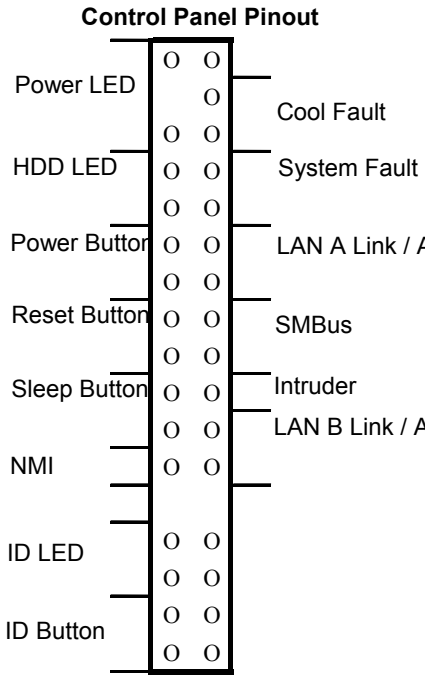


Figure 25. 34-Pin SSI Compliant Control Panel Header

7.5 I/O Connectors

7.5.1 VGA Connector

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

Table 94: VGA Connector Pin-out

Pin	Signal Name
1	Red (analog color signal R)
2	Green (analog color signal G)
3	Blue (analog color signal B)
4	No connection
5	GND
6	GND
7	GND
8	GND
9	Fused VCC (+5V)
10	GND
11	No connection

Pin	Signal Name
12	DDCDAT
13	HSYNC (horizontal sync)
14	VSYNC (vertical sync)
15	DDCCLK

7.5.2 NIC Connectors

The Server Board SE7520JR2 provides two RJ45 NIC connectors oriented side by side on the back edge of the board. The pin-out for each connector is identical and is defined in the following table:

Table 95: RJ-45 10/100/1000 NIC Connector Pin-out

Pin	Signal Name
1	
2	LAN_MID0P
3	LAN_MID0N
4	LAN_MID1P
5	LAN_MID2P
6	LAN_MID2N
7	LAN_MID1N
8	LAN_MID3P
9	LAN_MID3N
10	P2V5_NIC
11	LAN_LINK_1000_L (LED)
12	LAN_LINK_100_L_R (LED)
13	LAN_ACT_L (LED)
14	LAN_LINK_L_R (LED)
15	GND
16	GND

7.5.3 SCSI Connectors

The Server Board SE7520JR2 provides two SCSI connectors, one for each channel of the embedded LSI53C1030 SCSI controller. The external connector is routed to SCSI channel B, is a high density connector, and is found on the back edge of the server board. The internal connector is routed to SCSI channel A, is a standard 68 pin connector, and is located in the cut-out on the edge of the server board. The pin-out for each connector is identical and is defined in the following table.

Table 96: Internal/External 68-pin VHDCI SCSI Connector Pin-out

Pin#	Signal Name	Signal Name	Pin#
1	+DB(12)	-DB(12)	35

Pin#	Signal Name	Signal Name	Pin#
2	+DB(13)	-DB(13)	36
3	+DB(14)	-DB(14)	37
4	+DB(15)	-DB(15)	38
5	+DB(P1)	-DB(P1)	39
6	+DB(0)	-DB(0)	40
7	+DB(1)	-DB(1)	41
8	+DB(2)	-DB(2)	42
9	+DB(3)	-DB(3)	43
10	+DB(4)	-DB(4)	44
11	+DB(5)	-DB(5)	45
12	+DB(6)	-DB(6)	46
13	+DB(7)	-DB(7)	47
14	+DB(P)	-DB(P)	48
15	GROUND	GROUND	49
16	GROUND	GROUND	50
17	RESERVED	RESERVED	51
18	RESERVED	RESERVED	52
19	RESERVED	RESERVED	53
20	GROUND	GROUND	54
21	+ATN	-ATN	55
22	GROUND	GROUND	56
23	+BSY	-BSY	57
24	+ACK	-ACK	58
25	+RST	-RST	59
26	+MSG	-MSG	60
27	+SEL	-SEL	61
28	+C/D	-C/D	62
29	+REQ	-REQ	63
30	+I/O	-I/O	64
31	+DB(8)	-DB(8)	65
32	+DB(9)	-DB(9)	66
33	+DB(10)	-DB(10)	67
34	+DB(11)	-DB(11)	68

7.5.4 ATA-100 Connector

The Server Board SE7520JR2 provides one legacy ATA-100 40-pin connector (J3K1). The pin-out is defined in the following table. Its signals are not tied to the ATA functionality embedded into the high-density 100-pin front panel connector. Each connector is configured to a separate ATA port embedded in the ICH5-R.

Table 97: ATA-100 40-pin Connector Pin-out (J3K1)

Pin	Signal Name	Pin	Signal Name

Pin	Signal Name	Pin	Signal Name
1	RST_IDE_P_L	2	GND
3	IDE_PDD_7	4	IDE_PDD_8
5	IDE_PDD_6	6	IDE_PDD_9
7	IDE_PDD_5	8	IDE_PDD_10
9	IDE_PDD_4	10	IDE_PDD_11
11	IDE_PDD_3	12	IDE_PDD_12
13	IDE_PDD_2	14	IDE_PDD_13
15	IDE_PDD_1	16	IDE_PDD_14
17	IDE_PDD_0	18	IDE_PDD_15
19	GND	20	KEY
21	IDE_PDDREQ	22	GND
23	IDE_PDIOW_L	24	GND
25	IDE_PDIOR_L	26	GND
27	IDE_PIORDY	28	GND
29	IDE_PDDACK_L	30	GND
31	IRQ_IDE_P	32	Test Point
33	IDE_PDA1	34	IDE_CBL_DET_P
35	IDE_PDA0	36	IDE_PDA2
37	IDE_PDCS1_L	38	IDE_PDCS3_L
39	IDE_PRI_HD_ACT_L	40	GND

7.5.5 SATA Connectors

The Server Board SE7520JR2 provides two SATA (Serial ATA) connectors: SATA-0 (J1H1) and SATA-1 (J1H5), for use with an internal SATA backplane. The pin configuration for each connector is identical and is defined in the following table.

Table 98: SATA Connector Pin-out (J1H1 and J1H5)

Pin	Signal Name
1	GND1
2	S_ATA#_TX_P
3	S_ATA#_TX_N
4	GND2
5	S_ATA#_RX_N
6	S_ATA#_RX_P
7	GND3
8	GND4
9	GND5

7.5.6 Floppy Controller Connector

The following table details the pin-out of the 34-pin legacy floppy drive connector (J3K2). These signals are common to those used in the high-density 100-pin Front Panel connector. Concurrent use of these connectors is not supported.

Table 99: Legacy 34-pin Floppy Drive Connector Pin-out (J3K2)

Pin	Signal Name	Pin	Signal Name
1	GND	2	FD_DENSEL0
3	GND	4	Test Point
5	KEY	6	FD_DENSEL1
7	GND	8	FD_INDEX_L
9	GND	10	FD_MTR0_L
11	GND	12	FD_DS1_L
13	GND	14	FD_DS0_L
15	GND	16	FD_MTR1_L
17	Test Point	18	FD_DIR_L
19	GND	20	FD_STEP_L
21	GND	22	FD_WDATA_L
23	GND	24	FD_WGATE_L
25	GND	26	FD_TRK0_L
27	Test Point	28	VCC
29	GND	30	FD_RDATA_L
31	GND	32	FD_HDSEL_L
33	GND	34	FD_DSKCHG_L

7.5.7 Serial Port Connectors

The Server Board SE7520JR2 provides one external RJ45 Serial B port and one internal 9-pin Serial A header. The following tables define the pinouts for each.

Table 100: External RJ-45 Serial B Port Pin-out

Pin	Signal Name	Description
1	RTS	Request To Send
2	DTR	Data Terminal Ready
3	TXD	Transmit Data
4	GND	Ground
5	RI	Ring Indicate
6	RXD	Receive Data
7	DSR / DCD	Data Set Ready / Data Carrier Detect1
8	CTS	Clear To Send

Note:

1. A jumper block on the server board will determine whether DSR or DCD is routed to pin 7. The board will have the jumper block configured with DSR enabled at production.

Table 101: Internal 9-pin Serial A Header Pin-out (J1A3)

Pin	Signal Name
1	DCD (carrier detect)
2	DSR (data set ready)

3	RXD (receive data)
4	RTS (request to send)
5	TXD (Transmit data)
6	CTS (clear to send)
7	DTR (Data terminal ready)
8	RI (Ring Indicate)
9	Ground

7.5.8 Keyboard and Mouse Connector

Two stacked PS/2 ports are provided to support both a keyboard and a mouse. Either PS/2 port can support a mouse or keyboard. The following table details the pin-out of the PS/2 connector.

Table 102: Stacked PS/2 Keyboard and Mouse Port Pin-out

Pin	Signal Name
1	Keyboard Data
2	Test point – keyboard
3	GND
4	Keyboard / mouse power
5	Keyboard Clock
6	Test point – keyboard / mouse
7	Mouse Data
8	Test point – keyboard / mouse
9	GND
10	Keyboard / mouse power
11	Mouse Clock
12	Test point – keyboard / mouse
13	GND
14	GND
15	GND
16	GND
17	GND

7.5.9 USB Connector

The following table details the pin-out of the external USB connectors found on the back edge of the server board.

Table 103: External USB Connector Pin-out

Pin	Signal Name
1	USB_PWR
2	DATAL0 (Differential data line paired with DATAH0)
3	DATAH0 (Differential data line paired with DATAL0)

4	GND

One internal 1x10 connector on the baseboard (J1F1) provides an option to support an additional two USB 2.0 ports. This connector is used in both the Intel Server Chassis SR1400 1U and SR2400 2U bringing USB support to the control panel. The pin-out of the connector is detailed in the following table.

Table 104: Internal 1x10 USB Connector Pin-out (J1F1)

Pin	Signal name
1	USB_PWR(2)
2	USB_P2_L
3	USB_P2
4	Ground
5	Ground
6	USB_PWR(3)
7	USB_P3_L
8	USB_P3
9	Ground
10	Ground

For third party reference chassis, an internal 2x5 connector (J1G1) is supplied to provide an additional two USB ports. The pinout for this connector is found in the following table.

Table 105: Internal 2x5 USB Connector (J1G1)

Pin	Signal name
1	USB_PWR(5)
2	USB_PWR(4)
3	USB_BCK4_L
4	USB_BCK5_L
5	USB_BCK4
6	USB_BCK5
7	Ground
8	Ground
9	No Connect
10	No Connect

7.6 Fan Headers

The baseboard provides for several different system fan headers for use in Intel chassis as well as custom and third party reference chassis.

There are two SSI compliant processor fan headers, CPU1 (J7F1) and CPU2 (J5F2), which are not fan speed controlled. They are powered by a constant +12V. The pinout for these two connector is defined in the following table.

Table 106: CPU1/CPU2 Fan Connector Pin-out (J5F2, J7F1)

Pin	Signal Name	Type	Description
1	Fan Tach	Out	FAN_TACH signal is connected to the BMC to monitor the FAN speed
2	+12V	Power	Power Supply 12V
3	Ground	GND	GROUND is the power supply ground

The fan headers at J3K3 and J3K6 have fan speed control. Fan control is performed by two pulse width modulator (PWM) outputs on the LM93. The mBMC initializes the LM93 to control fan speeds based on temperature measurements according to a built-in table. The table itself is loaded as part of the SDR package according to which system configuration is used.

The 2x12 fan header (J3K6) is used to control system fans in both the Intel Server Chassis SR1400 and SR2400. The pinout for this connector is found in the following table.

Table 107: Intel Server Chassis Fan Header Pin-out (J3K6)

Pin	Signal Name	Type	Description
1	BB_FAN_LED4_R	IN	
2	BB_FAN_LED2_R	IN	
3	BB_FAN_LED3_R	IN	
4	BB_FAN_LED1_R	IN	
5	FAN_TACH8	OUT	FAN_TACH signal to monitor the FAN speed
6	FAN_TACH4	OUT	FAN_TACH signal to monitor the FAN speed
7	FAN_TACH7	OUT	FAN_TACH signal to monitor the FAN speed
8	FAN_TACH3	OUT	FAN_TACH signal to monitor the FAN speed
9	FAN_TACH6	OUT	FAN_TACH signal to monitor the FAN speed
10	FAN_TACH2	OUT	FAN_TACH signal to monitor the FAN speed
11	FAN_TACH5	OUT	FAN_TACH signal to monitor the FAN speed
12	FAN_TACH1	OUT	FAN_TACH signal to monitor the FAN speed
13	GROUND	GROUND	
14	GROUND	GROUND	
15	GROUND	GROUND	
16	GROUND	GROUND	
17	FAN_SPEED_CNTL_2	IN	Power supplied through fan speed control circuitry
18	FAN_SPEED_CNTL_1	IN	Power supplied through fan speed control circuitry
19	FAN_SPEED_CNTL_2	IN	Power supplied through fan speed control circuitry
20	FAN_SPEED_CNTL_2	IN	Power supplied through fan speed control circuitry
21	BB_FAN_LED7_R	IN	
22	BB_FAN_LED5_R	IN	
23	BB_FAN_LED8_R	IN	

24	BB_FAN_LED6_R	IN	

The 1x3 fan header (J3K3) is used to control a system fan in the Intel Server Chassis SR1400. The pinout for this connector is found in the following table.

Table 108: 3-Pin Fan Speed Controlled Fan Header (J3K3)

Pin	Signal Name	Type	Description
1	Fan Tach	Out	FAN_TACH signal is connected to the BMC to monitor the FAN speed
2	Fan_Speed_Cntl1	Power	Power supplied through fan speed control circuitry
3	Ground	GND	GROUND is the power supply ground

7.7 Misc. Headers and Connectors

7.7.1 Chassis Intrusion Header

A 1x2 pin header (J1A1) is used in chassis that support a chassis intrusion switch. This header is monitored by the mBMC. The pinout definition for this header is found in the following table.

Table 109: Chassis Intrusion Header (J1A1)

Pin	Signal Name	Description
1	FP_Chassis_Intr	
2	Ground	

7.7.2 Hard Drive Activity LED Header

A 1x2 pin header (J1A2) provides hard drive controller add-in cards an interface to the control panel Hard Drive Activity LED. The pinout definition for this header is found in the following table.

Table 110: Hard Drive Activity LED Header(J1A2)

Pin	Signal Name	Description
1	+3.3V	
2	FP_LED_L	

7.8 Jumper Blocks

The baseboard has several jumper blocks used to configure or enable/disable various features. This section describes the usage and settings of each.

Table 111: Jumper Block Definitions

Reference ID	Name	Description	Settings
J1H2 (A)	CMOS Clear	Clears CMOS settings	CMOS Clear by BMC – Pins 1-2 (Default) CMOS Clear Force Erase – Pins 2-3
J1H2 (B)	BIOS Recovery Boot	Forces the system to boot into BIOS Recovery mode. A bootable Recovery BIOS Floppy disk must be in Drive A for this operation.	Normal Boot - Pins 1-2 (Default) Enabled – Pins 2-3
J1H2 (C)	Password Clear	Clears Administrator and User passwords as set in BIOS Setup	Password Clr Protect – Pins 1-2 (Default) Password Clr Erase – Pins 2-3
J1A4	Rolling BIOS Configuration	Sets the BIOS flash device to boot from either the upper or lower banks of the flash device.	Normal Operation – Pins 1-2 (Default) Force to lower bank – Pins 2-3
J7A1	Serial B Configuration	Configures Pin 7 of the RJ45 Serial B port to support either a DCD or DSR signal	DCD Select –Pins 1-3 DSR Select – Pins 2-4 (Default)

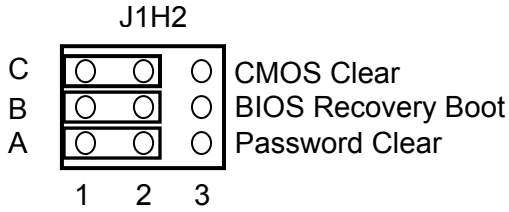


Figure 26. System Configuration (J1H2) Jumper Block Settings

8. Design and Environmental Specifications

8.1 Server Board SE7520JR2 Design Specification

Operation of the Server Board SE7520JR2 at conditions beyond those shown in the following table may cause permanent damage to the system. Exposure to absolute maximum rating conditions for extended periods may affect system reliability.

Table 112: Board Design Specifications

Operating Temperature	5º C to 50º C [1] (32º F to 131º F)
Non-Operating Temperature	-40º C to 70º C (-40º F to 158º F)
DC Voltage	± 5% of all nominal voltages
Shock (Unpackaged)	Trapezoidal, 50 g, 170 inches/sec
Shock (Packaged) (≥ 40 lbs to < 80 lbs)	24 inches
Vibration (Unpackaged)	5 Hz to 500 Hz 3.13 g RMS random

Note:
1. Chassis design must provide proper airflow to avoid exceeding Intel Xeon processor maximum case temperature.

Disclaimer Note: Intel Corporation server boards contain a number of high-density VLSI and power delivery components that need adequate airflow to cool. Intel ensures through its own chassis development and testing that when Intel server building blocks are used together, the fully integrated system will meet the intended thermal requirements of these components. It is the responsibility of the system integrator who chooses not to use Intel developed server building blocks to consult vendor datasheets and operating parameters to determine the amount of 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.

8.2 Power Supply Requirements

Note: The information provided in this section was derived from Intel's 500W power supply specification designed for use in the Server Chassis SR1400. The figures provided and the values in the tables are meant for reference purposes only and are based on a 1U rack server configuration. Variations in system configurations may produce different values.

8.2.1 Output Connectors

Listed or recognized component appliance wiring material (AVLV2), CN, rated min 105°C, 300Vdc shall be used for all output wiring.

Note: The following diagram shows the power harness spec drawing as defined for use in Intel server chassis. Reference chassis designs may or may not require all of the connectors shown and different wiring material may be needed to meet specific platform requirements.

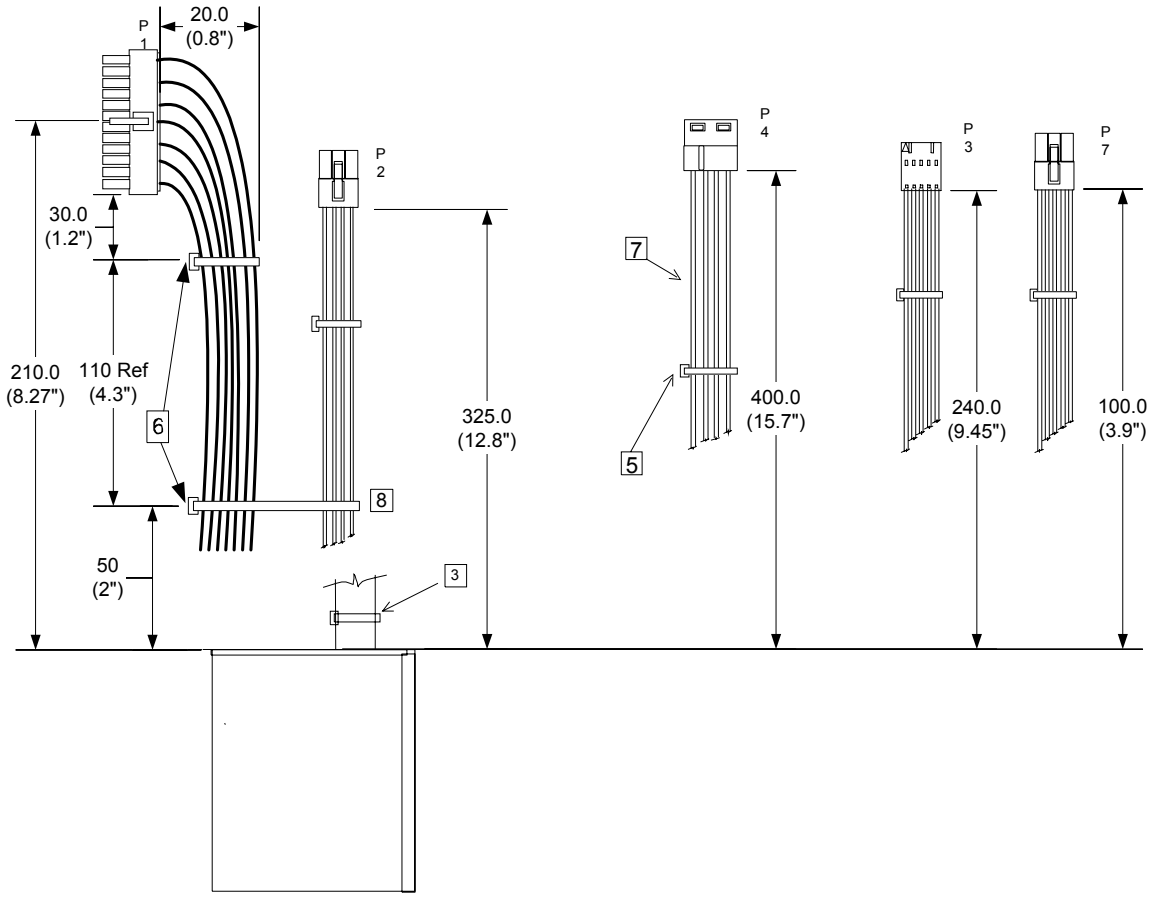


Figure 27. Power Harness Specification Drawing

Notes:

1. ALL DIMENSIONS ARE IN MM
2. ALL TOLERANCES ARE +10 MM / -0 MM
3. INSTALL 1 TIE WRAP WITHIN 12MM OF THE PSU CAGE
4. MARK REFERENCE DESIGNATOR ON EACH CONNECTOR
5. TIE WRAP EACH HARNESS AT APPROX. MID POINT
6. TIE WRAP P1 WITH 2 TIES AT APPROXIMATELY 15M SPACING.
7. P4 HARNESS IS ARESERVED FOR THE FUTURE ONLY, NO
8. PLEMENTATION IS NEEDED CURRENTLY.
9. TIE WRAP P1 AND P2 TOGETHER AT THIS POINT.

P1 Main Power Connector

- Connector housing: 24-pin Molex* Mini-Fit Jr. 39-01-2245 or equivalent
- Contact: Molex Mini-Fit, HCS, female, crimp 44476 or equivalent

Table 113: P1 Main Power Connector

Pin	SIgnal	18 AWG Color	Pin	SIgnal	18 AWG Color
1	+3.3 VDC	Orange	13	+3.3 VDC	Orange
2	+3.3 VDC	Orange	14	-12 VDC	Blue
3	COM	Black	15	COM	Black
4	+5 VDC*	Red	16	PSON#	Green
5	COM	Black	17	COM	Black
6	+5 VDC	Red	18	COM	Black
7	COM	Black	19	COM	Black
8	PWR OK	Gray	20	Reserved	N.C.
9	5VSB	Purple	21	+5 VDC	Red
10	+12V3	Yellow/Blue Stripe	22	+5 VDC	Red
11	+12V3	Yellow/Blue Stripe	23	+5 VDC	Red
12	+3.3 VDC	Orange	24	COM	Black

Notes:

- 5V Remote Sense Double Crimped into pin 4.
- 3.3V Locate Sense Double Crimped into pin 2.

P2 Processor Power Connector

- Connector housing: 8-pin Molex 39-01-2085 or equivalent
- Contact: Molex 44476-1111 or equivalent

Table 114: P2 Processor Power Connector

Pin	SIgnal	18 AWG Color	Pin	SIgnal	18 AWG Color
1	COM	Black	5	+12V1	Yellow
2	COM	Black	6	+12V1	Yellow
3	COM	Black	7	+12V2	Yellow/Black Stripe
4	COM	Black	8	+12V2	Yellow/Black Stripe

P3 Power Signal Connector

- Connector housing: 5-pin Molex 50-57-9705 or equivalent
- Contacts: Molex 16-02-0087 or equivalent

Table 115: P3 Baseboard Signal Connector

Pin	SIgnal	24 AWG Color
1	I2C Clock	White/Green Stripe
2	I2C Data	White/Yellow Stripe
3	Alert#	White
4	COM	Black
5	3.3RS	White/Brown Stripe

P4 Peripheral Connectors

- Connector housing: AMP V0 P/N is 770827-1 or equivalent
- Contact: Amp 61314-1 contact or equivalent

Table 116: Peripheral Power Connectors

Pin	SIgnal	18 AWG Color
1	+12 V3	Yellow/Blue Stripe
2	COM	Black
3	COM	Black
4	+5 VDC	Red

P7 Hard Drive Back Plane Power Connector

- Connector housing: 6-pin Molex Mini-Fit Jr. PN# 39-01-2065 or equivalent
- Contact: Molex Mini-Fit, HCS, female, crimp 44476 or equivalent

Table 117: P7 Hard Drive Power Connector

Pin	Signal	18 AWG Color
1	Ground	Black
2	Ground	Black
3	5V	Red
4	+12V3	Yellow/Blue Stripe
5	+12V3	Yellow/Blue Stripe
6	5VSB	Purple

8.2.2 Grounding

The ground of the pins of the power supply output connector provides the power return path. The output connector ground pins shall be connected to safety ground (power supply

enclosure). **This grounding must be designed to ensure passing the maximum allowed Common Mode Noise levels.**

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

8.2.3 Remote Sense

The power supply has remote sense return (ReturnS) to regulate out ground drops for all output voltages; +3.3V, +5V, +12V1, +12V2, +12V3, -12V, and 5VSB. The power supply uses remote sense (3.3VS) to regulate out drops in the system for the +3.3V output. The +5V, +12V1, +12V2, +12V3, –12V, and 5VSB outputs only use remote sense referenced to the ReturnS signal.

The remote sense input impedance to the power supply must be greater than 200Ω on 3.3VS, 5VS. This is the value of the resistor connecting the remote sense to the output voltage internal to the power supply. Remote sense must be able to regulate out a minimum of 200mV drop on the +3.3V output. The remote sense return (ReturnS) must be able to regulate out a minimum of 200mV drop in the power ground return. The current in any remote sense line shall be less than 5mA to prevent voltage sensing errors.

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

8.2.4 Standby Outputs

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

8.2.5 Voltage Regulation

The power supply output voltages must stay within the following voltage limits when operating at steady state and dynamic loading conditions. These limits include the peak-peak ripple/noise. All outputs are measured with reference to the return remote sense signal (ReturnS). The 5V, 12V1, 12V2, +12V3, –12V and 5VSB outputs are measured at the power supply connectors referenced to ReturnS. The +3.3V is measured at it remote sense signal (3.3VS) located at the signal connector.

Table 118: Voltage Regulation Limits

Parameter	Tolerance	Minimum	Nominal	Maximum	Units
+ 3.3V	- 5% / +5%	+3.14	+3.30	+3.46	V_{rms}
+ 5V	- 5% / +5%	+4.75	+5.00	+5.25	V_{rms}
+ 12V1	- 5% / +5%	+11.40	+12.00	+12.60	V_{rms}
+ 12V2	- 5% / +5%	+11.40	+12.00	+12.60	V_{rms}
+ 12V3	- 5% / +5%	+11.40	+12.00	+12.60	V_{rms}
- 12V	- 5% / +9%	-11.40	-12.00	-13.08	V_{rms}
+ 5VSB	- 5% / +5%	+4.75	+5.00	+5.25	V_{rms}

8.2.6 Dynamic Loading

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

Table 119: Transient Load Requirements

Output	Δ Step Load Size (See note 2)	Load Slew Rate	Test Capacitive Load
+3.3V	5.0A	0.25 A/μsec	250 μF
+5V	4.0A	0.25 A/μsec	400 μF
12V1+12V2+12V3	20.0A	0.25 A/μsec	2200 μF [1, 3]
+5VSB	0.5A	0.25 A/μsec	20 μF

Notes

1. Step loads on each 12V output may happen **simultaneously**.
2. For Load Range 2 (light system loading), the tested step load size should be 60% of those listed.
3. The +12V should be tested with 1000μF evenly split between the three +12V rails.

8.2.7 Capacitive Loading

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

Table 120: Capacitve Loading Conditions

Output	MIN	MAX	Units
+3.3V	**250**	6,800	μF
+5V	**400**	4,700	μF
+12V(1, 2, 3)	**500 each**	11,000	μF
-12V	**1**	350	μF
+5VSB	**20**	350	μF

8.2.8 Closed Loop Stability

The power supply shall be unconditionally stable under all line/load/transient load conditions including capacitive load ranges. A minimum of: **45 degrees phase margin** and **-10dB-gain margin** is required. Closed-loop stability must be ensured at the maximum and minimum loads as applicable.

8.2.9 Common Mode Noise

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

8.2.10 Ripple / Noise

The maximum allowed ripple/noise output of the power supply is defined in the following table. This is measured over a bandwidth of 0Hz to 20MHz at the power supply output connectors.

Table 121: Ripple and Noise

+3.3V	+5V	+12V1/2	-12V	+5VSB
50mVp-p	50mVp-p	120mVp-p	120mVp-p	50mVp-p

8.2.11 Soft Starting

The power supply shall contain control circuit that provides monotonic soft start for its outputs without overstress of the AC line or any power supply components at any specified AC line or load conditions. There is no requirement for rise time on the 5V Standby but the turn on/off shall be monotonic.

8.2.12 Zero Load Stability Requirements

When the power subsystem operates in a no load condition, it does not need to meet the output regulation specification, but it must operate without any tripping of over-voltage or other fault circuitry. When the power subsystem is subsequently loaded, it must begin to regulate and source current without fault. Each output voltage may not be internally diode isolated. At the same time failure in the primary side of one power supply doesn't cause the other to shut down.

8.2.13 Timing Requirements

These are the timing requirements for the power supply operation. The output voltages must rise from 10% to within regulation limits (T_{vout_rise}) within 5 to 70ms, except for 5VSB - it is allowed to rise from 1.0 to 70ms. The +3.3V, +5V and +12V output voltages should start to rise approximately at the same time**. All outputs must rise monotonically**. The +5V output needs to be greater than the +3.3V output during any point of the voltage rise. The +5V output must never be greater than the +3.3V output by more than 2.25V. Each output voltage shall reach regulation within 50ms (T_{vout_on}) of each other during turn on of the power supply. Each output voltage shall fall out of regulation within 400msec (T_{vout_off}) of each other during turn off. The following figures show the timing requirements for the power supply being turned on and off via the AC input, with PSON held low and the PSON signal, with the AC input applied.

Table 122: Output Voltage Timing

Item	Description	Minimum	Maximum	Units
T_{vout_rise}	Output voltage rise time from each main output.	**5.0 ***	**70 ***	msec
T_{vout_on}	All main outputs must be within regulation of each other within this time.		**50**	msec
T_{vout_off}	All main outputs must leave regulation within this time.		**400**	msec

Note:

The 5VSB output voltage rise time shall be from 1.0ms to 25.0ms

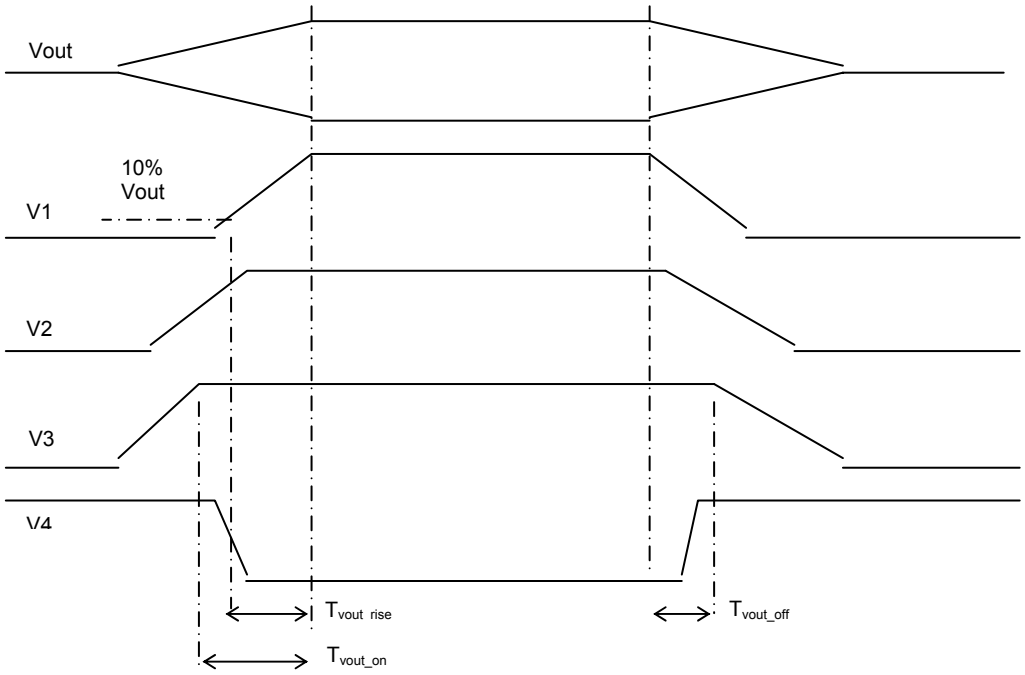


Figure 28. Output Voltage Timing

Table 123: Turn On/Off Timing

Item	Description	Minimum	Maximum	Units
$T_{sb\_on\_delay}$	Delay from AC being applied to 5VSB being within regulation.		**1500**	msec
$T_{ac\_on\_delay}$	Delay from AC being applied to all output voltages being within regulation.		**2500**	msec
T_{vout_holdup}	Time all output voltages stay within regulation after loss of AC.	**21**		msec
T_{pwok_holdup}	Delay from loss of AC to de-assertion of PWOK	**20**		msec
$T_{pson\_on\_delay}$	Delay from PSON# active to output voltages within regulation limits.	**5**	**400**	msec
T_{pson_pwok}	Delay from PSON# deactive to PWOK being de-asserted.		**50**	msec
T_{pwok_on}	Delay from output voltages within regulation limits to PWOK asserted at turn on.	**100**	**1000**	msec
T_{pwok_off}	Delay from PWOK de-asserted to output voltages (3.3V, 5V, 12V, -12V) dropping out of regulation limits.	**1**		msec
T_{pwok_low}	Duration of PWOK being in the de-asserted state during an off/on cycle using AC or the PSON signal.	**100**		msec
T_{sb_vout}	Delay from 5VSB being in regulation to O/Ps being in regulation at AC turn on.	**50**	**1000**	msec
T_{5VSB_holdup}	Time the 5VSB output voltage stays within regulation after loss of AC.	**70**		msec

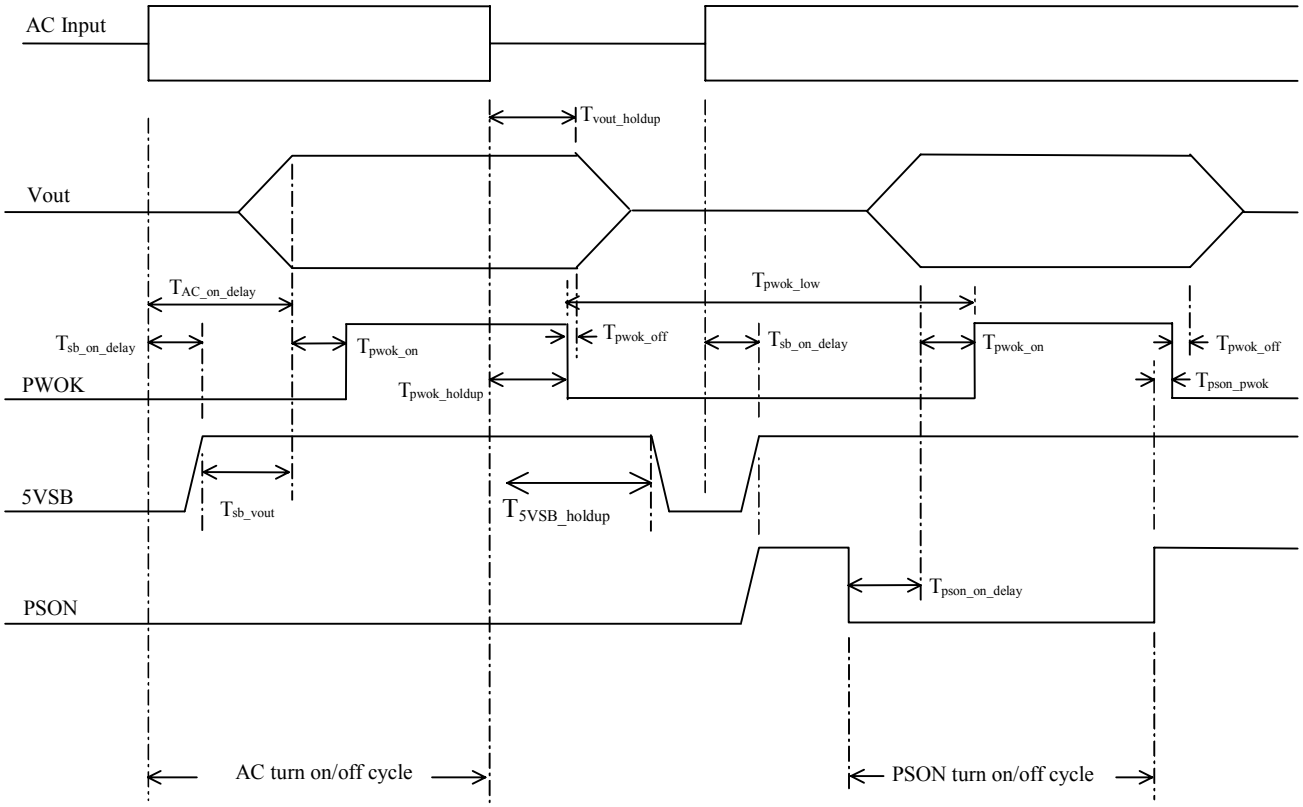


Figure 29. Turn On/Off Timing (Power Supply Signals)

8.2.14 Residual Voltage Immunity in Standby Mode

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

The residual voltage at the power supply outputs for no load condition shall not exceed 100mV when AC voltage is applied.

8.3 Product Regulatory Compliance

8.3.1 Product Safety Compliance

The Server Board SE7520JR2 complies with the following safety requirements:

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

8.3.2 Product EMC Compliance – Class A Compliance

Note: Legally the product is required to comply with Class A emission requirements as it is intended for a commercial type market place. Intel targets 10db margin to Class A Limits

The Server Board SE7520JR2 has been has been tested and verified to comply with the following electromagnetic compatibility (EMC) regulations when installed a compatible Intel® host system. For information on compatible host system(s) refer to Intel's Server Builder Web site or contact your local Intel representative.

- FCC /ICES-003 - Emissions (USA/Canada) Verification
- CISPR 22 – Emissions (International)
- EN55022 - Emissions (Europe)
- EN55024 - Immunity (Europe)
- CE – EMC Directive 89/336/EEC (Europe)
- AS/NZS 3548 Emissions (Australia / New Zealand)
- BSMI CNS13438 Emissions (Taiwan)
- GOST R 29216-91 Emissions - Listed on one System License (Russia)
- GOST R 50628-95 Immunity –Listed on one System License (Russia)
- Belarus License – Listed on one System License (Belarus)
- RRL MIC Notice No. 1997-41 (EMC) & 1997-42 (EMI) (Korea)

8.3.3 Certifications / Registrations / Declarations

- UL Certification (US/Canada)
- CE Declaration of Conformity (CENELEC Europe)
- FCC/ICES-003 Class A Attestation (USA/Canada)
- C-Tick Declaration of Conformity (Australia)
- MED Declaration of Conformity (New Zealand)
- BSMI Certification (Taiwan)
- GOST – Listed on one System License (Russia)
- Belarus – Listed on one System License (Belarus)
- RRL Certification (Korea)
- Ecology Declaration (International)

8.3.4 Product Regulatory Compliance Markings

This product is marked with the following Product Certification Markings:

Table 124: Product Certification Markings

Regulatory Compliance	Country	Marking
UL Mark	USA/Canada	
CE Mark	Europe	
FCC Marking (Class A)	USA	This device complies with Part 15 of the FCC Rules. Operation of this device is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation. Manufactured by Intel Corporation
EMC Marking (Class A)	Canada	CANADA ICES-003 CLASS A CANADA NMB-003 CLASSE A
BSMI Marking (Class A)	Taiwan	 警告使用者： 這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策
RRL MIC Mark	Korea	

8.4 Electromagnetic Compatibility Notices

8.4.1 FCC (USA)

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

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

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

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

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

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

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

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

8.4.2 Industry Canada (ICES-003)

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

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

8.4.3 Europe (CE Declaration of Conformity)

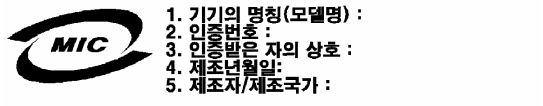
This product has been tested in accordance too, and complies with the Low Voltage Directive (73/23/EEC) and EMC Directive (89/336/EEC). The product has been marked with the CE Mark to illustrate its compliance.

8.4.4 Taiwan Declaration of Conformity (BSMI)

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

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

8.4.5 Korean Compliance (RRL)



English translation of the notice above:

Type of Equipment (Model Name): On License and Product

Certification No.: On RRL certificate. Obtain certificate from local Intel representative

Name of Certification Recipient: Intel Corporation

Date of Manufacturer: Refer to date code on product

Manufacturer/Nation: Intel Corporation/Refer to country of origin marked on product

9. Miscellaneous Board Information

9.1 Updating the System Software

To ensure your Server Board SE7520JR2 has the latest board fixes, it is highly recommended to load the latest system software. These include System BIOS, mBMC firmware, and FRUSDR Utility. It may also include Intel Management Module (IMM) BMC Firmware (if installed) and Hot Swap Controller (HSC) firmware if the baseboard is installed into an Intel server chassis with a backplane. The latest system software for the Server Board SE7520JR2 can be downloaded from the following Intel web site:

http://support.intel.com/support/motherboards/server/se7520jr2/

You can use the Server Menu in the <F2> BIOS Utility to verify what versions of system software are installed on your server. If you determine that an update is necessary, the system software should be updated in the following order:

- HSC firmware (If Applicable)
- mBMC Firmware
- IMM BMC Firmware (If Applicable)
- FRUSDR Utility
- System BIOS

It is highly recommended to read the README.TXT file that accompanies each update package for complete install instructions and release notes before attempting to update the system software onto your server board.

9.2 Programming FRU and SDR Data

Regardless of which platform management option is being used, On-board Platform Instrumentation or Intel Management Module, the baseboard must have the proper Sensor Data Records (SDR) and Field Replaceable Unit (FRU) data programmed to the board.

The FRUSDR Update Utility is an application used to program the platform management sub-system to monitor the proper platform sensors. This application is provided on the Intel Server Deployment Toolkit CDROM that comes with the baseboard or can be downloaded from the following Intel Website:

http://support.intel.com/support/motherboards/server/se7520jr2/

The FRUSDR Update Utility should be run prior to loading any OS or Server Management Software. The FRUSDR Update Utility determines which chassis the baseboard is integrated into, which FRUs are present, and programs the Platform Management Sub-system to monitor the proper platform sensors accordingly. The FRUSDR Update Utility must be run when the board is first integrated into a platform and must be run when the system configuration is changed as follows:

- Adding/Removing an IMM

- Replacing a bad baseboard
- Adding/Removing a Redundancy Feature (IMM Systems Only)
    - Redundant Power Supplies
    - Redundant Fans
- Adding/Removing a CPU fan (IMM Systems Only)

Failure to run the FRUSDR Update Utility may cause the platform management sub-system to report false errors causing your platform to operate erratically.

Note: It is highly recommended that you update your Server Board SE7520JR2 with the latest system software, including the FRUSDR Update Utility. These can be downloaded from the following Intel web site: http://support.intel.com/support/motherboards/server/se7520jr2/

9.3 Clearing CMOS

Depending on which System Management level is used on the server, there are three possible methods that can be used to clear the system CMOS:

- System Configuration Jumper Block J1H2 (A) - CMOS Clear Jumper - Supported with all management levels
- Control Panel CMOS clear sequence (IMM Professional and Advanced system only)
- *CMOS Clear* state asserted via BMC *CMOS Clear Options* command (allows remote clear operation) (Professional and Advanced systems Only)

9.3.1 CMOS Clear Using J1H2 Jumper Block

All three management levels support clearing the CMOS using by moving the CMOS Clear jumper of the System Config jumper block (J1H2- A) from the default position pins 1-2 to pin position 2-3. This method requires the following procedure to be followed:

1. The power be removed from the system
2. The J1H2 jumper is moved
3. The system is rebooted.
4. BIOS Setup options are saved
5. System is powered down and AC is removed
6. Jumper J1H2 is moved back to default position
7. AC is restored
8. System is rebooted.

9.3.2 CMOS Clear using Control Panel

In systems configured with an Intel Management Module, Professional or Advanced, CMOS can be cleared using buttons on the system Control Panel that will both assert the BMC *CMOS*

Clear state and power the system up. This feature can be enabled or disabled via the *CMOS Clear Options* command.

The following sequence of events must occur to invoke the Control Panel CMOS Clear feature.

1. Standby power must be on, system power must be off, and the feature enabled.
2. The control panel reset button must be pressed and held for at least 4 seconds
3. With the control panel reset button still pressed, the control panel power button must be pressed

The IMM Sahalee BMC produces a single beep through the system speaker to confirm the CMOS clear button sequence.

The Sahalee BMC does not assert the CMOS Clear hardware signal. BIOS checks for BMC CMOS Clear state (using the *CMOS Clear Options* command) at each boot to determine if the Sahalee BMC is requesting a CMOS Clear operation. The BMC CMOS Clear state remains active until one of the following events occurs:

It is forced off using a *CMOS Clear Options* command (this is the normal operational case, by BIOS).
The reset button is pressed.
The power button is pressed and released.
The system is powered off.

9.4 BIOS Recovery Operation

The BIOS Recovery Operation should be attempted if for any reason the BIOS gets corrupted causing the system to hang at POST generating a CMOS error. Should the system exhibit POST hangs due to BIOS corruption, you should:

Option 1) cycle power.

This option will perform 1 of 2 possible operations. The reboot may clear possible BIOS corruption with the Primary BIOS image and the system will boot normally. If the Primary BIOS image is non-correctable, the system will perform an Auto Recovery which loads the secondary or backup BIOS image. If this option is not successful and your system continues to exhibit CMOS corruption errors, you can attempt option 2.

Option 2)

- Obtain BIOS Update Package From the following Intel Web Site: :http://support.intel.com/support/motherboards/server/se7520jr2/
- Turn off the system
- Verify the jumper on jumper block J1A4 is set to Pins 1-2.
- Build Recovery Storage Media using files compressed in the RECOVERY.ZIP file
- Recovery from USB Disk-on-key or other large media
    - Prepare a formatted and bootable storage media device such as a USB DISK_ON_KEY.
    - Copy AMIBOOT.ROM to it.

- Recovery from multiple floppy disks.
    - Prepare 2 blank disks.
    - The first disk(disk0) must be made bootable
    - Copy amiboot.000 to disk0, and amiboot.001 to disk1.
- Execute BIOS Recovery
    - set Recovery Boot Jumper by moving jumper J1H2 row B from Pins 1-2 to Pins 2-3
    - Insert the recovery media to the appropriate drive or USB interface.
    - Power on system
    - The System will automatically boot to the media and start the BIOS recovery operation.
    - During multi-disk recovery operation, system will beep (1sec) continuously
    - to notify user to insert disk1
    - When the update has completed, the system will beep 4 times, followed by an endless beep.
    - Turn off the system and unplug it.
    - set jumper J1H2 back to Normal mode J1H2 B(1-2).
- Recovery operation complete.

Appendix A: Integration and Usage Tips

The following Integration and Usage Tips are provided to assist with answering miscellaneous questions about the Server Board SE7520JR2 or as a guide to assist with troubleshooting common errors.

- The use of DDR2 - 400 MHz or DDR - 266/333 MHz DIMMs is dependant on which board SKU is used. DDR-2 DIMMs cannot be used on a board designed to support DDR. DDR DIMMs cannot be used on boards designed to support DDR-2
- DDR-266 & DDR-333 DIMM population rules are as follows:
  A. DIMM banks must be populated in order starting with the slots furthest from MCH
  B. Single rank DIMMs must be populated before dual rank DIMMs
  C. A maximum of four DIMMs can be populated when all four DIMMs are dual rank DDR-333 DIMMs.
- DDR2-400 DIMM population rules are as follows:
  A. DIMMs banks must be populated in order starting with the slots furthest from MCH
  B. Dual rank DIMMs are populated before single rank DIMMs
  C. A maximum of four DIMMs can be populated when all four DIMMs are dual rank DDR2-400 DIMMs
- On the Server Board SE7520JR2, when using all dual rank DDR-333 or DDR2-400 DIMMs, a total of four DIMMs can be populated. Configuring more than four dual rank DDR-333 or DDR2-400 DIMMs will result in the BIOS generating a memory configuration error
- The DIMM Sparing feature requires that the spare DIMM be at least the size of the largest primary DIMM in use
- It is possible for a Memory RASUM feature to be initiated without notification that the action has occurred when using standard on-board platform instrumentation
- A ZCR card is only supported on the full-height riser slot. When installing the card, it MUST be populated in the PCI-X add-in slot furthest from the baseboard.
- The Server Board SE7520JR2 has support for Zero Channel RAID (ZCR) which follows the RUBI2 standard. It will not have support for zero channel RAID cards that follow the RADIOS standard.
-

Glossary

This appendix contains important terms used in the preceding chapters. 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.

Term	Definition
ACPI	Advanced Configuration and Power Interface
AP	Application Processor
APIC	Advanced Programmable Interrupt Control
ASIC	application specific integrated circuit
BIOS	Basic input/output system
BIST	Built-in self test
BMC	Sahalee Baseboard Management Controller
Bridge	Circuitry connecting one computer bus to another, allowing an agent on one to access the other.
BSEL	
BSP	Bootstrap processor
byte	8-bit quantity.
CBC	Chassis bridge controller. A microcontroller connected to one or more other CBCs. Together they bridge the IPMB buses of multiple chassis.
CEK	Common Enabling Kit
CHAP	Challenge Handshake Authentication Protocol
CMOS	In terms of this specification, this describes the PC-AT compatible region of battery-backed 128 bytes of memory, which normally resides on the baseboard.
DPC	Direct Platform Control
EEPROM	Electrically erasable programmable read-only memory
EHCI	Enhanced Host Controller Interface
EMP	Emergency management port.
EPS	External Product Specification
FMB	Flexible Mother Board
FMC	Flex Management Connector
FMM	Flex Management Module
FRB	Fault resilient booting
FRU	Field replaceable unit
FSB	Front side Bus
GB	1024 MB.
GPIO	General purpose I/O
GTL	Gunning Transistor Logic
HSC	Hot-swap controller
Hz	Hertz (1 cycle/second)
I2C	Inter-integrated circuit bus
IA	Intel® architecture
IBF	Input buffer
ICH	I/O controller hub
ICMB	Intelligent Chassis Management Bus
IERR	Internal error

Term	Definition
IFB	I/O and firmware bridge
IMM	Intel Management Module
INTR	
IP	Internet Protocol
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
IR	Infrared
ITP	In-target probe
KB	1024 bytes.
KCS	Keyboard controller style
LAN	Local area network
LCD	Liquid crystal display
LED	Light Emitting Diode
LPC	Low pin count
LUN	Logical unit number
MAC	Media Access Control
MB	1024 KB
mBMC	National Semiconductor© PC87431x mini BMC
MCH	Memory Controller Hub
MD2	Message Digest 2 – Hashing Algorithm
MD5	Message Digest 5 – Hashing Algorithm – Higher Security
Ms	milliseconds
MTTR	Memory Tpe Range Register
Mux	multiplexor
NIC	Network interface card
NMI	Nonmaskable interrupt
OBF	Output buffer
OEM	Original equipment manufacturer
Ohm	Unit of electrical resistance
PEF	Platform event filtering
PEP	Platform event paging
PIA	Platform Information Area – This feature configures the firmware for the platform hardware.
PLD	programmable logic device
PMI	Platform management interrupt
POST	Power-on Self Test
PSMI	Power Supply Management Interface
PWM	Pulse-width Modulation
RAM	Random Access Memory
RASUM	Reliability, availability, serviceability, usability, and manageability
RISC	Reduced instruction set computing
ROM	Read Only Memory
RTC	Real-time clock. Component of ICH peripheral chip on the baseboard.
SDR	Sensor data record
SECC	Single edge connector cartridge

Term	Definition
SEEPROM	Serial electrically erasable programmable read-only memory
SEL	System Event Log
SIO	Server Input/output
SMI	Server management interrupt. SMI is the highest priority nonmaskable interrupt.
SMM	Server management mode.
SMS	Server management software
SNMP	Simple Network Management Protocol.
TBD	To Be Determined
TBSG	
TIM	Thermal Interface Material
UART	universal asynchronous receiver/transmitter
UDP	User Datagram Protocol.
UHCI	Universal Host Controller Interface
UTC	Universal time coordinare
VID	Voltage Identification
VRD	Voltage Regulator Down
Word	16-bit quantity
ZIF	Zero Insertion Force

Reference Documents

Refer to the following documents for additional information:

- Intel® Server Board SE7520JR2 Server Management External Architecture Specification (EAS). Intel Corporation.
- Intel® Server Board SE7520JR2 BIOS External Product Specification. Intel Corporation
- Intel® Server Board SE7520JR2 BMC External Product Specification. Intel Corporation
- Mini Baseboard Management Controller mBMC Core External Product Specification. Intel Corporation
- Silverwood Server Management Firmware External Architecture Specification (EAS). Intel Corporation.
- Intel Server Chassis SR1400 and SR2400 Technical Product Specification, Intel Corporation.
- Sahalee Baseboard Management Controller Core External Product Specification (Sahalee BMC Core EPS for IPMI 2.0 Systems), Intel Corporation.
- Sahalee Platform Information Area External Product Specification (Sahalee PIA EPS) ver 1.0, Intel Corporation
- Advanced Configuration and Power Interface Specification. Intel Corporation, Microsoft Corporation, Toshiba Corporation.
- Intelligent Chassis Management Bus (ICMB) Specification, Version 1.0. Intel Corporation, Hewlett-Packard Company, NEC Corporation, Dell Computer Corporation.
- Intelligent Platform Management Bus Communications Protocol Specification, Version 1.0. 1998. Intel Corporation, Hewlett-Packard Company, NEC Corporation, Dell Computer Corporation.
- Intelligent Platform Management Interface Specification, Version 2.0. Intel Corporation, Hewlett-Packard Company, NEC Corporation, Dell Computer Corporation.
- Platform Management FRU Information Storage Definition. 1998. Intel Corporation, Hewlett-Packard Company, NEC Corporation, Dell Computer Corporation. http://developer.intel.com/design/servers/ipmi/spec.htm
- The I^2C Bus and How to Use It, January 1992. Phillips Semiconductors.
- Power Supply Management Interface (PSMI), Revision 1.4, 2003. Intel Corporation