Intel® Server Boards SE7320SP2 and SE7525GP2

Technical Product Specification

Intel reference number D24635-004

Revision 4.0

December, 2005

Enterprise Platforms and Services Division - Marketing

Revision History

Date	Revision Number	Modifications
June 2004	1.0	Initial Release
November 2004	2.0	Updated and clarified memory support, removed LX SKU references, added MTBF calculations, performed general grammar and spelling updates.
September 2005	3.0	Updated supported processors matrix and BIOS setup options according to new BIOS release, modified front panel pin-out description, updated the function introduction of Wake on LAN from S5
December 2005	4.0	Added the introduction of CME counter in the section “3.5.4 – Disabling DIMMs”, added the tip of fan configuration when integrated in third-party chassis

Disclaimers

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

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

The Intel® Server Boards SE7320SP2 and SE7525GP2 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.

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.

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

1. Introduction

This Technical Product Specification (TPS) provides detail to the architecture and feature set of the Intel® Server Board SE7320SP2 and the Intel® Server Board SE7525GP2. Unless otherwise noted, features discussed in this document apply to both server boards.

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.

1.1 Chapter Outline

This document is divided into the following chapters

- Chapter 1: Introduction
- Chapter 2: Server Board Overview
- Chapter 3: Functional Architecture
- Chapter 4: System BIOS
- Chapter 5: Platform Management
- Chapter 6: Error Reporting and Handling
- Chapter 7: Connector Definitions and Pin-outs
- Chapter 8: General Specifications
- Chapter 9: Product Regulatory Compliance

1.2 Server Board Use Disclaimer

Intel Corporation server boards contain a number of high-density VLSI and power delivery components which 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 can not be held responsible, if components fail or the server board does not operate correctly when used outside any of their published operating or non-operating limits.

2. Server Board Overview

The Intel® Server Boards SE7320SP2 and SE7525GP2 are monolithic printed circuit boards with features that were designed to support the entry-level server market. The Server Board SE7525GP2 has features that also make it suitable for the workstation market. The features of both boards will be discussed in detail in this document. Unless otherwise noted, features discussed in this document apply to both server boards.

2.1 Intel® Server Board SE7320SP2

One SKU of the Intel® Server Board SE7320SP2 is available. This product is based on the Intel® E7320 chipset and provides an interface to a single PCI Express* bus, one 32-bit / 33-MHz PCI bus and one 64-bit / 66-MHz PCI-X* bus. Additionally, integrated on the board is a gigabit NIC and an ATI* Rage XL video solution. A detailed list of the features is listed below.

2.1.1 Intel® Server Board SE7320SP2 Feature Set

- Dual processor slots supporting Intel® Xeon® processors operating at 800MT/s system bus
- Intel® E7320 chipset (MCH, 6300ESB)
- Four DIMM slots supporting DDR 266/333 MHz memory
- Single Intel® 82541 10/100/1000 Network Interface controller (NIC)
- Onboard ATI* Rage XL video controller with 8 MB SDRAM
- Intel® Server Management support
- External I/O connectors
- Stacked PS2 ports for keyboard and mouse
- DB-9 Serial A Port
- RJ-45 NIC connector
- 15-pin video connector
- Two USB 2.0 ports
- Internal I/O connectors / headers
- Onboard USB port headers (capable of supporting two USB ports)
- DH10 Serial B header
- Two SATA-150 connectors with integrated chipset RAID 0/1 support
- Two ATA100 connectors
- Floppy connector
- SSI compliant front panel headers
- SSI compliant 24-pin main power connector (supports ATX 12V standard in first 20 pins)
- Internal expansion connectors
- One x8 PCI Express* connector (on x4 PCI Express bus)
- Two 32-bit / 33-MHz PCI connectors
- Two 64-bit / 66-MHz PCI-X* connectors
- Intel® Light-Guided Diagnostics on some FRU devices (processors, memory)
- Port 80 Diagnostic LEDs displaying POST codes

The following figure shows the board layout of the Intel® Server Board SE7320SP2. Each connector and major component is identified by number and identified in Table 1.

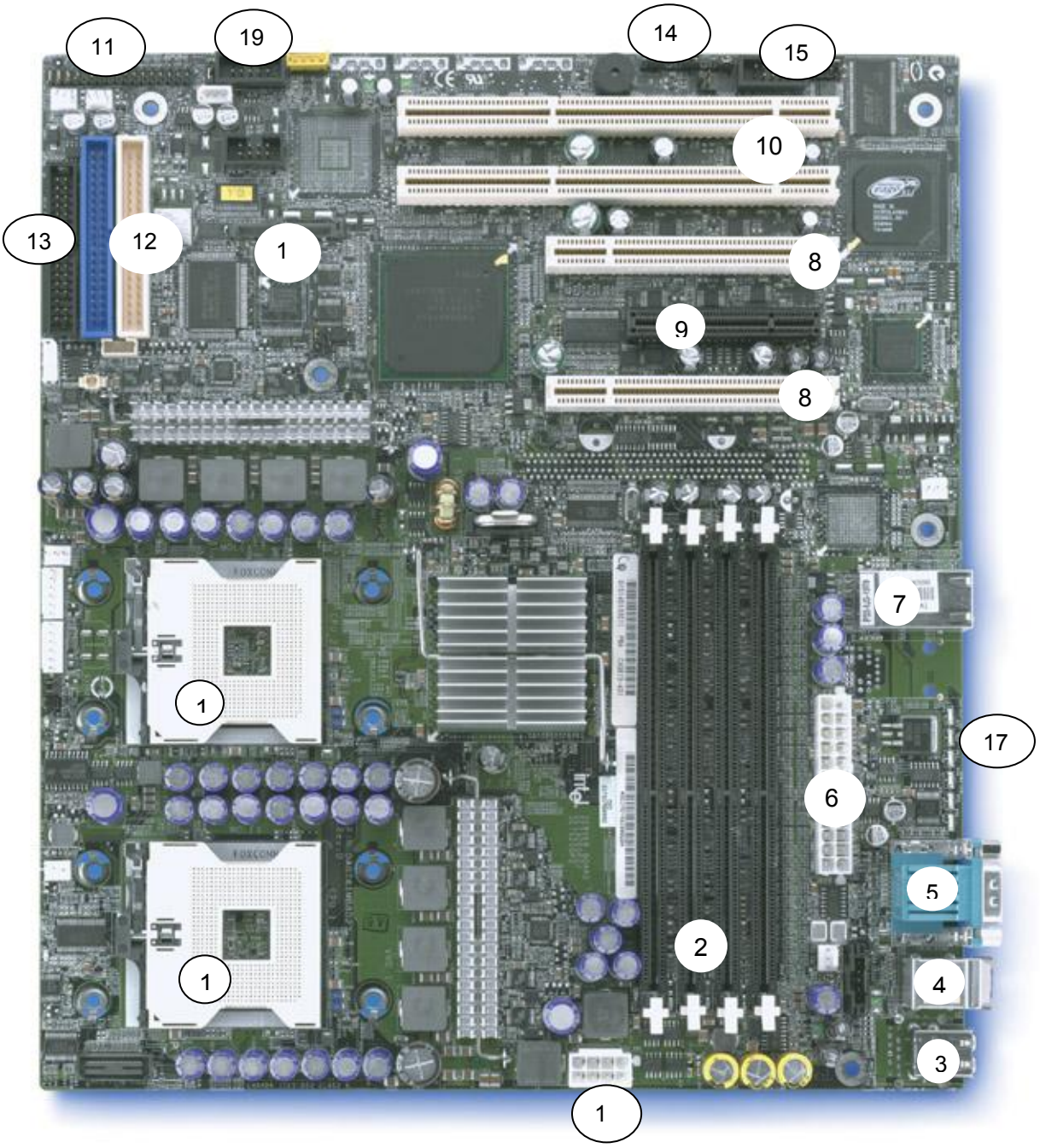


Figure 1. Intel® Server Board SE7320SP2 Layout

Table 1. Intel® Server Board SE7320SP2 Layout Reference

Ref #	Description	Ref #	Description
1	Processor sockets	11	Front panel header
2	DIMM connectors (from left to right 2A, 2B, 1A, 1B)	12	PATA HDD connectors (primary = blue, secondary = white)
3	Two external USB connectors	13	Floppy connector
4	Keyboard and mouse connector	14	Main jumper block
5	Stacked video and serial	15	Serial B header
6	Main power	16	12V CPU power
7	RJ-45 gigabit NIC connector	17	Post Code LEDs
8	32-bit PCI slots	18	SATA connectors (left to right A2, A1)
9	PCI Express* x8 connector (x4 bus)	19	Front panel USB header
10	PCI-X* 64-bit 66 MHz		

2.2 Intel® Server Board SE7525GP2

One SKU of the Server Board SE7525GP2 is available. This section describes its feature set. While similar to the Server Board SE7320SP2, there are specific features that make this server board suitable for an entry-level workstation solution as well as an entry-server environment.

2.2.1 Intel® Server Board SE7525GP2 Feature Set

- Dual processor slots supporting Intel® Xeon® processors operating on the 800MT/s system bus
- Intel® E7525 chipset (MCH, ICH5R)
- Four DIMM slots supporting DDR-266/333 MHz memory
- One Intel® 82541 10/100/1000 Network Interface controller (NIC)
- Onboard ATI* Rage XL video controller with 8-MB SDRAM
- Intel® Server Management support
- External I/O connectors
- Stacked PS2 ports for keyboard and mouse
- DB-9 Serial A port
- RJ-45 NIC connector
- 15-pin video connector
- Two USB 2.0 ports
- Internal I/O connectors / headers
- Onboard USB port headers (capable of supporting two USB ports)
- DH10 Serial B header
- Two SATA-150 connectors with integrated chipset RAID 0/1 support
- Two ATA100 connectors
- Floppy connector

- SSI-compliant front panel headers
- SSI-compliant 24-pin main power connector (will support ATX-12V standard in first 20 pins)
- Internal expansion connectors
- One x16 PCI Express* graphics connector
- One x 8 PCI Express connector (on x4 PCI Express bus)
- Two 32-bit / 33-MHz PCI connectors
- Two 64-bit / 66-MHz PCI-X* connectors
- Intel® Light-Guided Diagnostics on most FRU devices (processors, memory)
- Port-80 diagnostic LEDs displaying POST Codes

The following figure shows the board layout of the Intel® Server Board SE7525GP2. Each connector and major component is identified by number and identified in Table 2.

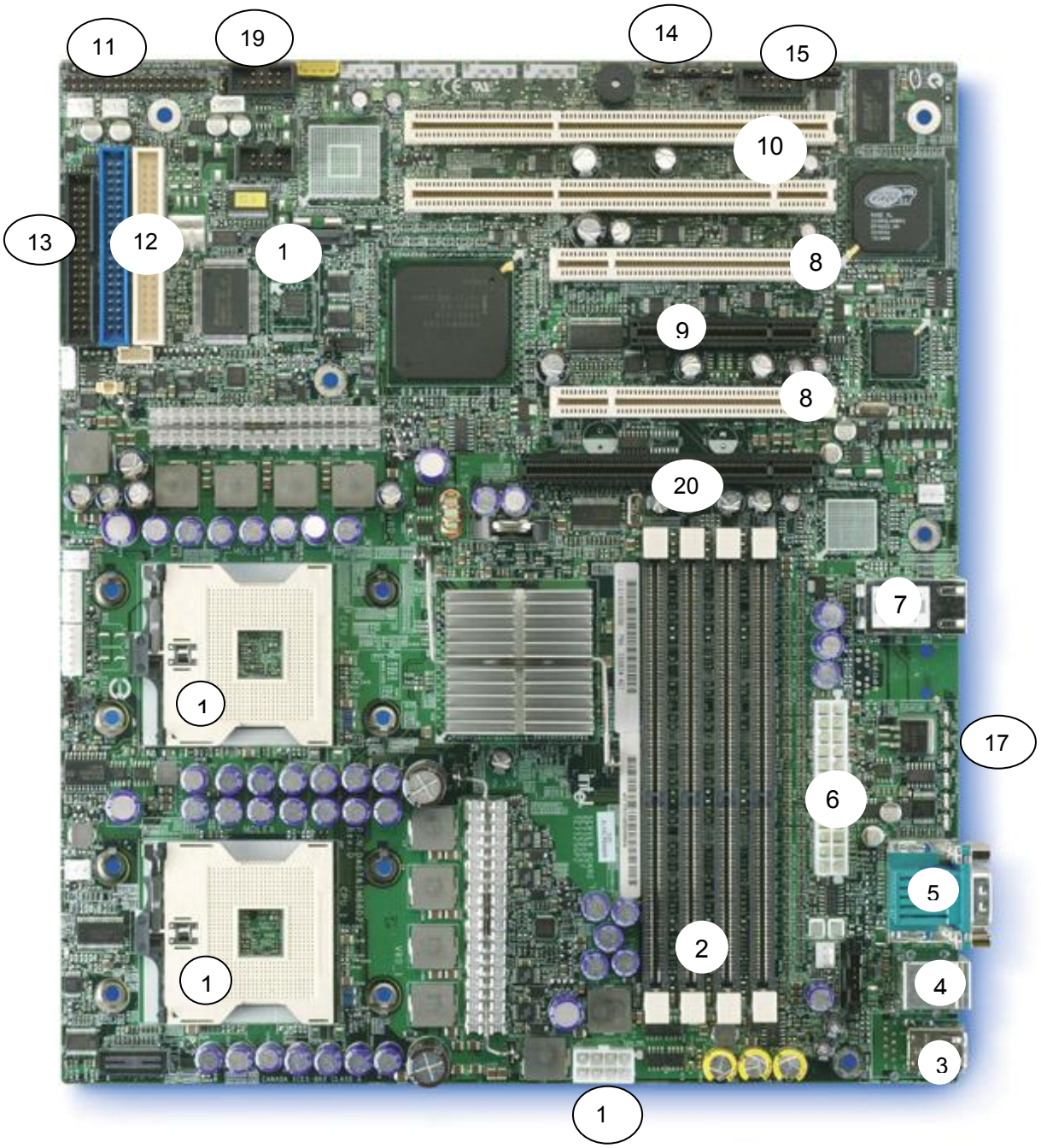


Figure 2. Intel® Server Board SE7525GP2 Layout

Table 2. Intel® Server Board SE7525GP2 Layout Reference

Ref #	Description	Ref #	Description
1	Processor sockets	11	Front panel header
2	DIMM connectors (from left to right 2A, 2B, 1A, 1B)	12	PATA HDD connectors (primary = blue, secondary = white)
3	Two external USB connectors	13	Floppy connector
4	Keyboard and mouse connector	14	Main jumper block
5	Stacked video and serial	15	Serial B header
6	Main power	16	12V CPU power
7	RJ-45 Gigabit NIC connector	17	Post Code LEDs
8	32-bit PCI slots	18	SATA connectors (left to right A2, A1)
9	PCI Express* x8 connector (x4 bus)	19	Front panel USB header
10	PCI-X* 64-bit / 66-MHz	20	PCI Express x16 connector

3. Functional Architecture

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

Note: *Due to the similarities between these two products, this chapter discusses all features that are present on both products. Where appropriate, features that are specific to one product or the other will noted.*

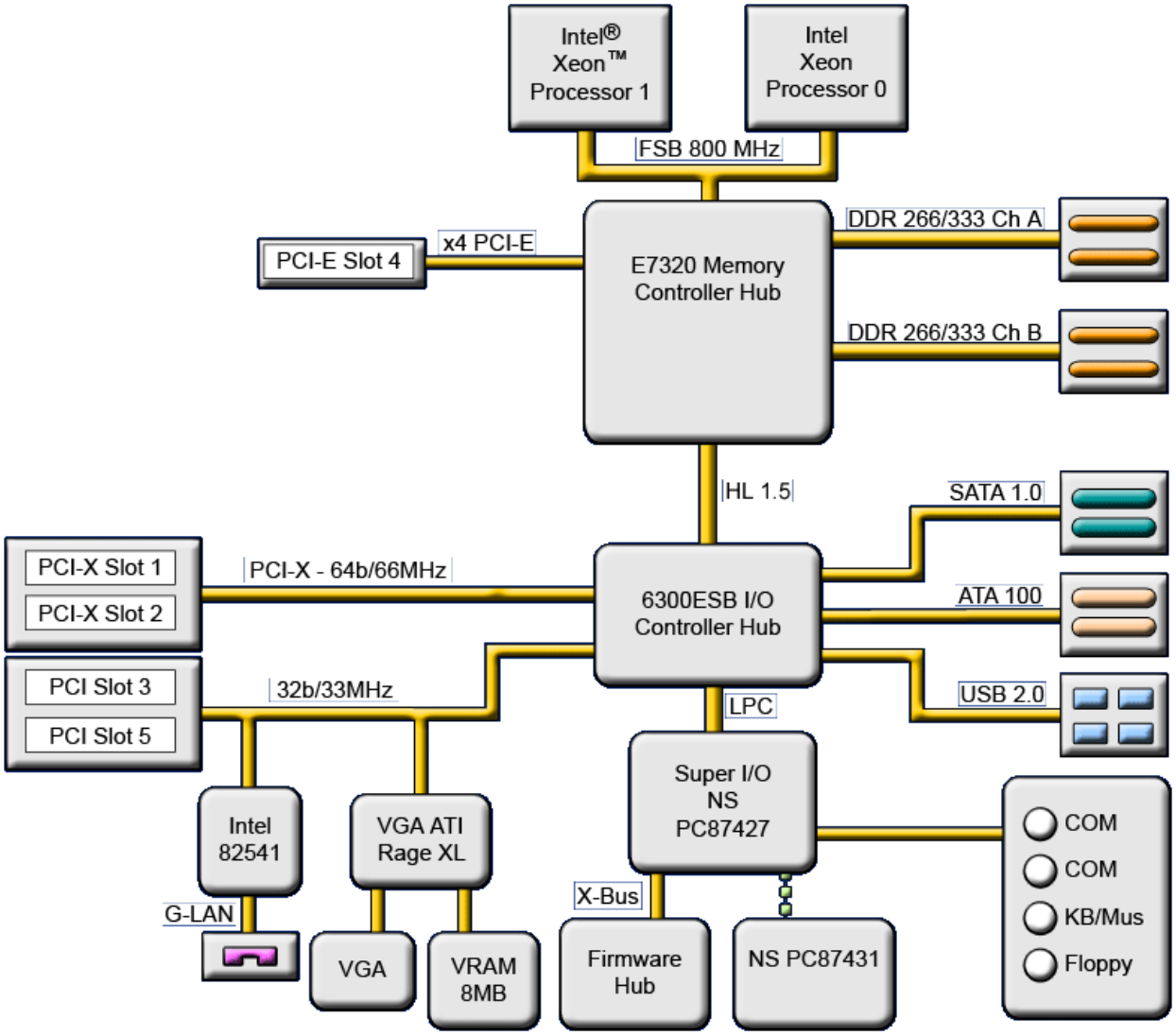


Figure 3. Intel® Server Board SE7320SP2 Block Diagram

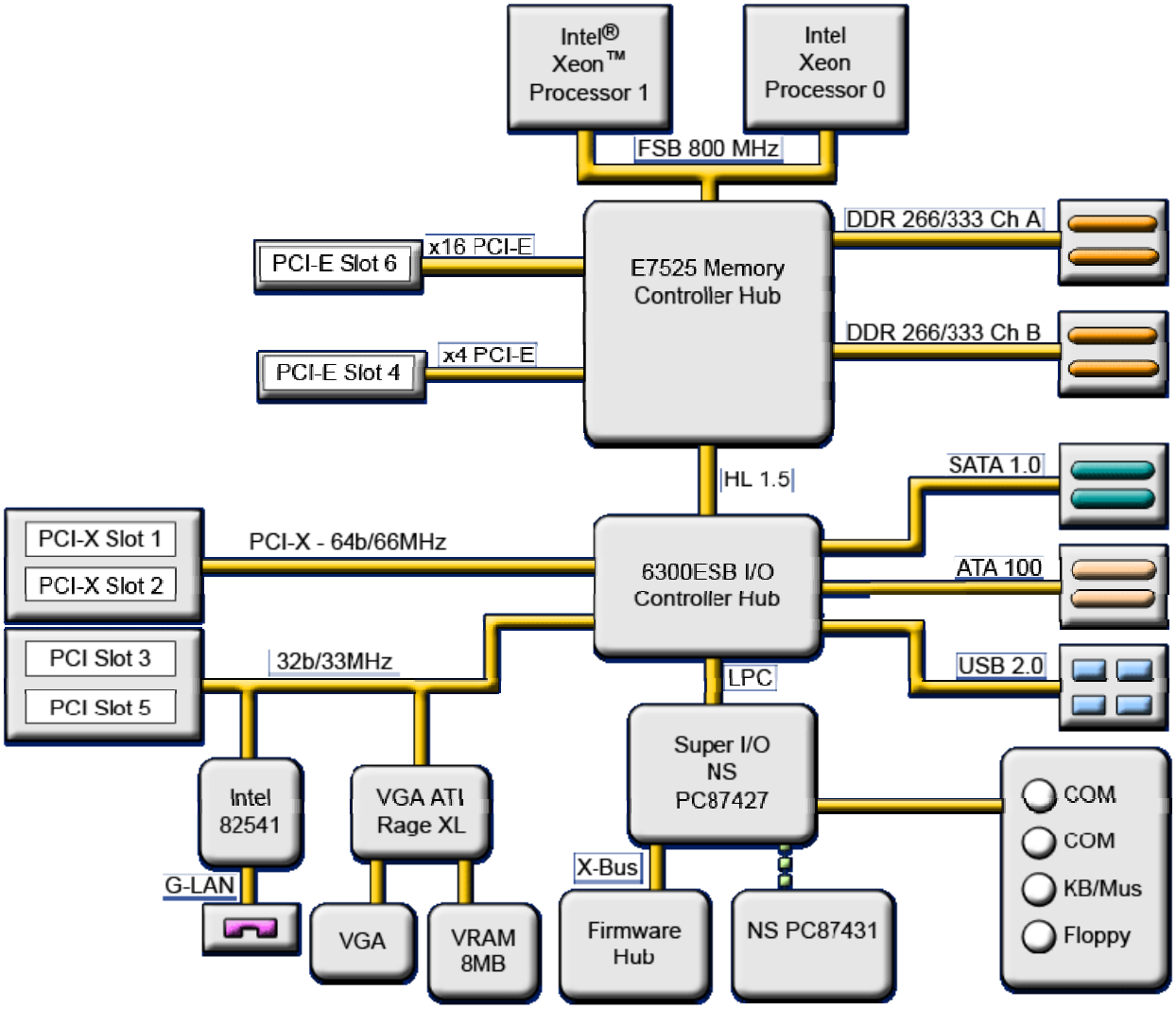


Figure 4. Intel® Server Board SE7525GP2 Block Diagram

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 Regulator Devices (VRDs)

The server board has two voltage regulator devices (VRDs) that provide 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 current of 105 amps and peak support of 120 amps.

The server boards support the flexible motherboard (FMB) specification for all 800-MHz FSB Intel® Xeon® processors with respect to current requirements and processor speed requirements. 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

The server boards provide logic to detect the presence and identity of installed processors. In dual processor configurations, the onboard 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 server board ensures that the following criteria are met:

- In a uni-processor configuration, processor 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 server board has been designed to comply with Intel's common enabling kit (CEK) processor mounting and heatsink retention solution. The server board will ship with a CEK spring snapped onto the underside of the board, beneath each processor socket. The CEK spring is removable, allowing for the use of non-Intel heatsink retention solutions.

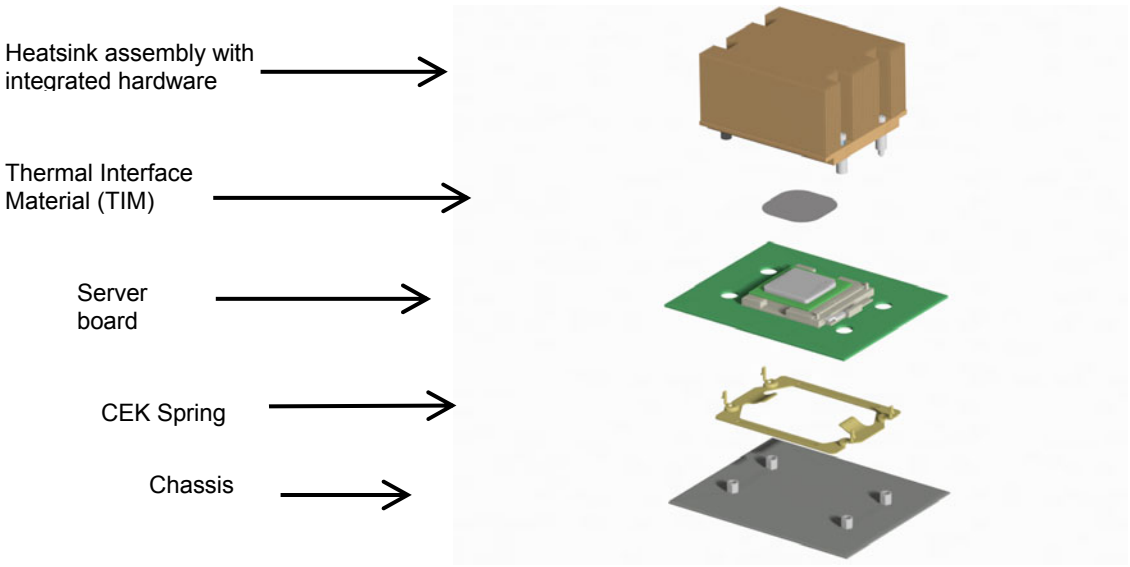


Figure 5. CEK Processor Mounting

3.1.6 Processor Support

The server boards are 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 processors are not supported on either of these server boards.

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

Note: *Only Intel® Xeon® processors that support an 800-MHz front side bus are supported on these server boards. See the table below for the supported processors.*

Table 3. 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
Intel Xeon	800 MHz	3.2 GHz	Yes
Intel Xeon	800 MHz	3.4 GHz	Yes
Intel Xeon	800 MHz	3.6 GHz	Yes
Intel Xeon	800 MHz	3.8 GHz	Yes

Note: *The latest BIOS needs to be implemented before to have new Intel® Xeon® processors supported on these server boards.*

See the Supported Processors List located on the support website for a complete list of supported processors.

http://support.intel.com/support/motherboards/server/se7320sp2

http://support.intel.com/support/motherboards/server/se7525gp2

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. Server board 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 the standard onboard platform instrumentation, the mBMC will log an error against processor 1 to the system event log and the server board hardware will light both processor error LEDs.

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 one stepping difference between them. If the installed processors are more than one stepping apart, an error is reported. Acceptable mixed steppings are not reported as errors by the BIOS.

3.1.6.3 Mixed Processor Models

Processor models cannot be mixed in a system. If this condition is detected, error 8196 is logged in the SEL.

3.1.6.4 Mixed Processor Families

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

3.1.6.5 Mixed Processor Cache Sizes

If the installed processors have mixed cache sizes, error 8192 will be logged in the SEL. 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 boot strap processor (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 the 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. The BIOS Setup utility 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) 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 Intel® Extended Memory 64 Technology (Intel® EM64T) Support

The system BIOS supports the Intel® Extended Memory 64 technology (Intel® EM64T) feature of the Intel® Xeon® processors. There is no BIOS setup option to enable or disable this support. The system is in IA-32 compatibility mode when booting to an operating system. Operating system specific drivers are loaded to enable this capability.

3.1.6.12 Execute Disable Bit support

The system BIOS supports the execute-disable (NX) bit in the latest Intel® Xeon® processors. This option can be enabled or disabled in the BIOS setup utility. It is disabled by default to allow users to opt-in to the protection this feature provides.

3.1.7 Multiple Processor Initialization

IA-32 processors have a microcode-based boot strap processor (BSP) arbitration protocol. On reset, all of the processors compete to become the BSP. If a serious error is detected during a 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 wakes each application processor (AP). When awakened, an AP programs its memory type range registers (MTRRs) to be identical to those of the BSP. All APs execute a halt instruction with their 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 by the thermal diodes. These are monitored by the LM93* device. The mBMC configures the LM93 device 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 indicating throttling due to thermal conditions. The mBMC implements an IPMI sensor that provides the percentage of time a processor has been throttling over the last 1.46 seconds. Server 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) an Intel® Xeon® processor outputs a digital signal that is monitored by the server board 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 it will assert the System Status LED and generate an event in the system event log.

3.1.11 Processor IERR

The IERR signal is asserted by the Intel® Xeon® processor as a result of an internal error. The mBMC configures the heceta7 device to monitor this signal. When this signal is asserted, the mBMC generates a processor IERR event.

3.2 Intel® E7320 Chipset (Intel® Server Board SE7320SP2)

The architecture of the Intel® Server Board SE7320SP2 is designed around the Intel® E7320 chipset. The Intel® Server Board SE7525GP2 is designed around the Intel® E7525 chipset. This is discussed in the next section.

The Intel® E7320 chipset is a subset of the Intel® E7520 chipset and consists of two components that together are responsible for providing the interface between all major sub-systems found on the server board, including the processor, memory, and I/O sub-systems. These components are:

- Memory controller hub (MCH)
- I/O controller hub (Intel® 6300ESB)

The following sub-sections provide an overview, describing the primary functions and supported features of each chipset component. Later sections discuss how these features are implemented on the Server Board SE7320SP2.

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 Intel® E7320 MCH supports either single- or dual-processor configurations using Intel® Xeon® processors designed for the 800 MHz system bus. 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 Intel® E7320 MCH provides an integrated memory controller for direct connection to two channels of registered DDR266, DDR333 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.

When both DDR channels are populated and operating, they function in lock-step mode. For the Intel® E7320 MCH, the maximum supported memory size at DDR266, DDR333 or DDR2-400 memory configuration is 12 GB. On the Intel® Server Board SE7320SP2, the maximum supported memory size at DDR266 or DDR333 is 8 GB. DDR2-400 memory is not supported on this server board.

There are several RASUM (reliability, availability, serviceability, usability, and manageability) features built into the Intel® E7320 MCH memory interface:

- DIMM sparing allows for one DIMM per channel to be held in reserve and brought on-line if another DIMM in the channel becomes defective.
- Hardware periodic memory scrubbing, including demand scrub support.
- Retry on uncorrectable memory errors.
- x4 SDDC (Single Device Data Correction) 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 Intel® E7320 MCH is part of the first family of Intel chipsets to support the PCI Express* high speed serial I/O interface for high I/O bandwidth. The Intel E7320 MCH implementation of the scalable PCI Express interface complies with the *PCI Express Interface Specification, Rev 1.0a*. The E7320 MCH provides one configurable x8 PCI Express interface with a maximum theoretical bandwidth of 4 GB/s. The x8 PCI Express interface may alternatively be configured (bifurcated) as two independent x4 PCI Express interfaces. On the Server Board SE7320SP2, the PCI Express bandwidth is divided between two independent PCI Express buses; one operating at x4 for add-in cards, and one embedded on the board for possible future upgradeability.

The Intel® E7320 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. See the *SE7320SP2/SE7525GP2 Tested Hardware and OS List* for the adapters tested on those systems.

3.2.1.4 Hub Interface

The MCH interfaces with the Intel® 6300ESB I/O controller hub through a dedicated hub interface that supports a peak bandwidth of 266 MB/s using a x4 base clock of 66 MHz. The 6300ESB I/O controller is discussed in further detail later in this document.

3.3 Intel® E7525 Chipset (Intel® Server Board SE7525GP2)

The architecture of the Server Board SE7525GP2 is designed around the Intel® E7525 chipset. The Server Board SE7320SP2 is designed around the E7320 chipset and was discussed in the previous section.

The Intel E7525 chipset is a subset of the Intel® E7520 chipset and consists of two components that together are responsible for providing the interface between all major sub-systems found on the server board including the processor, memory, and I/O sub-systems. These components are the:

- Memory controller hub (MCH)
- I/O controller hub (Intel® 6300ESB)

The following sub-sections provide an overview, describing the primary functions and supported features of each chipset component. Later sections discuss how these features are implemented on the Server Board SE7525GP2.

3.3.1 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

3.3.1.1 Front Side Bus (FSB)

The Intel® E7525 MCH supports either single- or dual-processor configurations using Intel® Xeon® processors designed for the 800-MHz system bus. 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.

3.3.1.2 MCH Memory Sub-System Overview

The Intel® E7525 MCH provides an integrated memory controller for direct connection to two channels of registered DDR266, DDR333 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.

When both DDR channels are populated and operating, they function in lock-step mode. For the Intel E7525 MCH, the maximum supported memory size at DDR266, DDR333 or DDR2-400 is 12 GB. On the Server Board SE7525GP2, the maximum supported memory size at DDR266 or DDR333 is 8 GB. DDR2-400 memory is not supported on this server board.

There are several RASUM (reliability, availability, serviceability, usability, and manageability) features built into the Intel E7525 MCH memory interface:

- DIMM sparing allows for one DIMM per channel to be held in reserve and brought on-line if another DIMM in the channel becomes defective.
- Hardware periodic memory scrubbing, including demand scrub support.
- Retry on uncorrectable memory errors.
- x4 SDDC (Single Device Data Correction) for memory error detection and correction of any number of bit failures in a single x4 memory device.

3.3.1.3 PCI Express*

The Intel® E7525 MCH is part of the first family of Intel chipsets to support the PCI Express* high speed serial I/O interface for high I/O bandwidth. The Intel E7525 MCH implementation of the scalable PCI Express interface complies with the *PCI Express Interface Specification, Rev 1.0a*. The MCH provides one x16 and one configurable x8 PCI Express interface with a maximum theoretical bandwidth of 4 GB/s. The x8 PCI Express interface may alternatively be configured (bifurcated) as two independent x4 PCI Express interfaces. On the Server Board SE7525GP2, the PCI Express bandwidth is implemented as one x16 slot for high bandwidth PCI Express graphics adapters and one x4 slot for PCI Express add-in cards.

The Intel® E7525 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. See the *SE7320SP2 / SE7525GP2 Tested Hardware and OS List* for the add-in cards tested on this platform.

3.3.1.4 Hub Interface

The MCH interfaces with the Intel® 6300ESB I/O controller hub via a dedicated hub Interface supporting a peak bandwidth of 266 MB/s using a x4 base clock of 66 MHz.

3.4 Intel® 6300ESB ICH

The Intel® 6300ESB is a multi-function device that provides 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.
- PCI-X 2.2 specification support for up to PCI-X 66 MHz operation
- 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 four 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 Intel® 6300ESB I/O controller 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.

3.4.1 PCI Interface

The Intel® 6300ESB I/O controller PCI interface provides a 33-MHz, Revision 2.3-compliant implementation. All PCI signals are 5-V tolerant, except for PME#. The Intel 6300ESB I/O controller integrates a PCI arbiter that supports up to four external PCI bus masters in addition to the internal Intel 6300ESB requests. This PCI interface is used to support onboard PCI devices including the ATI* video controller, Intel® 82541 Gigabit NIC, and the Super I/O chip.

The Intel 6300ESB I/O controller hub provides a 64-bit/66 MHz revision 2.2 compliant PCI-X implementation. The bus is also PCI 2.2 compliant to provide backwards compatibility with PCI devices. The Intel 6300ESB ICH also works as the PCI arbiter on this bus and supports up to four external PCI bus masters in addition to the Intel 6300ESB I/O controller. Two 3.3V PCI-X connectors are on this bus.

3.4.2 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 any ISA DMA resources. The IDE interface integrates 16x32-bit buffers for optimal transfers. The Intel® 6300ESB I/O controller 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).

3.4.3 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 Intel® 6300ESB I/O controller 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.

3.4.4 Low Pin Count (LPC) Interface

The Intel® 6300ESB I/O controller 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 Intel 6300ESB I/O controller 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.

3.4.5 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 Intel® 6300ESB I/O controller supports two types of DMA (LPC and PC/PCI). LPC DMA and PC/PCI DMA use the Intel 6300ESB I/O controller 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 Intel 6300ESB I/O controller provides an ISA-compatible programmable interrupt controller (PIC) that incorporates the functionality of two 82C59 interrupt controllers. The two interrupt controllers are cascaded so that 14 external and two internal interrupts are possible. In addition, the Intel 6300ESB I/O controller 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.

3.4.6 Advanced Programmable Interrupt Controller (APIC)

In addition to the standard ISA-compatible PIC described in the previous section, the Intel® 6300ESB I/O controller incorporates the advanced programmable interrupt controller (APIC).

3.4.7 Universal Serial Bus (USB) Controller

The Intel® 6300ESB I/O controller contains an *Enhanced Host Controller Interface Specification for Universal Serial Bus, Revision 1.0*-compliant host controller that supports USB high-speed signaling. High-speed USB 2.0 allows data transfers up to 480 Mb/s which is 40 times faster than full-speed USB. The Intel 6300ESB I/O controller also contains four universal host controller interface (UHCI) controllers that support USB full-speed and low-speed signaling. On the Intel® Server Board SE7320SP2, the Intel 6300ESB I/O controller supports four USB 2.0 ports. All four ports are high-speed, full-speed, and low-speed capable. Intel 6300ESB I/O controller port-routing logic determines whether a USB port is controlled by one of the UHCI controllers or by the EHCI controller.

3.4.8 RTC

The Intel® 6300ESB I/O controller contains the 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 also 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 also supports a date alarm that allows for scheduling a wake-up event up to 30 days in advance.

3.4.9 GPIO

Various general purpose inputs and outputs are provided for custom system design. The number of inputs and outputs varies depending on the Intel® 6300ESB I/O controller configuration. All unused GPI pins must be pulled high or low, so that they are at a predefined level and do not cause undue side effects.

3.4.10 Enhanced Power Management

The Intel® 6300ESB I/O controller power management functions include enhanced clock control, local and global monitoring support for 14 individual devices, and various low-power (suspend) states (e.g., Suspend-to-DRAM and Suspend-to-Disk). A hardware-based thermal management circuit permits software-independent entrance to low-power states. The Intel 6300ESB I/O controller contains full support for the Advanced Configuration and Power Interface (ACPI) Specification, Revision 2.0b.

3.4.11 System Management Bus (SMBus 2.0)

The Intel® 6300ESB I/O controller contains an SMBus Host interface that allows the processor to communicate with SMBus slaves. This interface is compatible with most I2C devices. Special I2C commands are implemented. The Intel 6300ESB I/O controller SMBus host controller provides a mechanism for the processor to initiate communications with SMBus peripherals (slaves). Also, the Intel 6300ESB I/O controller supports slave functionality, including the Host Notify protocol. Hence, the host controller supports eight command protocols of the SMBus interface (see System Management Bus (SMBus) Specification, Version 2.0): Quick Command, Send Byte, Receive Byte, Write Byte/Word, Read Byte/Word, Process Call, Block Read/Write, and Host Notify.

3.5 Memory Sub-System

The MCH provides an integrated memory controller for direct connection to two channels of registered DDR266 or DDR333 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.

When both DDR channels are populated and operating, they function in lock-step mode. The maximum supported memory size for either memory speed is 8 GB.

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.

3.5.1 Memory Sizing

The server boards provide four DDR266 / DDR333 DIMM sites. There are two DIMM sites on each memory channel.

DIMMs on channel A are paired with DIMMs on channel B to configure 2-way interleaving. The minimum memory configuration to support interleaving is two DIMMs, which requires same DIMM populated from each channel. Each board does support single-channel memory operation with a single DIMM populated in DIMM location 1 on either bank (1A or 2A). It should be noted that single-channel operation greatly reduces memory bandwidth and RAS capabilities.

Memory DIMM technologies supported are: 128 Mb, 256 Mb, 512 Mb, 1 Gb and 2 Gb.

Physical DIMM sizes supported are 256 MB, 512 MB, 1 GB, and 2 GB.

See the Tested Memory List on the support website for a list of supported memory:

http://support.intel.com/support/motherboards/server/se7320sp2

http://support.intel.com/support/motherboards/server/se7525gp2

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 row of DIMMs. The BIOS programs the Memory controller in the chipset accordingly. The total amount of configured memory can be found using BIOS Setup.

The DIMM pair, which constitutes interleaving, 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 pair are single-sided, only one row is said to be present in the system. For double-sided DIMMs, both rows are said to be present.

For interleaving and RAS to be enabled, memory DIMMs must be populated in pairs. The server boards each have four DIMM slots, or two 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.

3.5.2 Memory Population

The mixing of memory DDR266 and DDR333 is supported on Server Board SE7320SP2 and Server Board SE7525GP2. However, when mixing DIMM speeds, DDR333 will be treated as DDR266.

DIMM search rules for standard mode:

1. If DIMM dual pair# >= 1, set memory controller to dual-channel mode. Otherwise, go to step 2.

2. If Channel A DIMM is present, set memory controller to single-channel mode A. Otherwise, go to step 3.

3. If Channel B DIMM is present, set memory controller to single-channel mode B. Otherwise, memory configuration error.

The DIMM population rules are as follows:

- DIMMs should be populated starting from the bank furthest from the MCH – DIMM slots 1A and 1B.
- Starting with Bank 1, mixed DIMMs must be populated by single rank, then dual rank.

The following diagram identifies the memory bank locations on the server board.

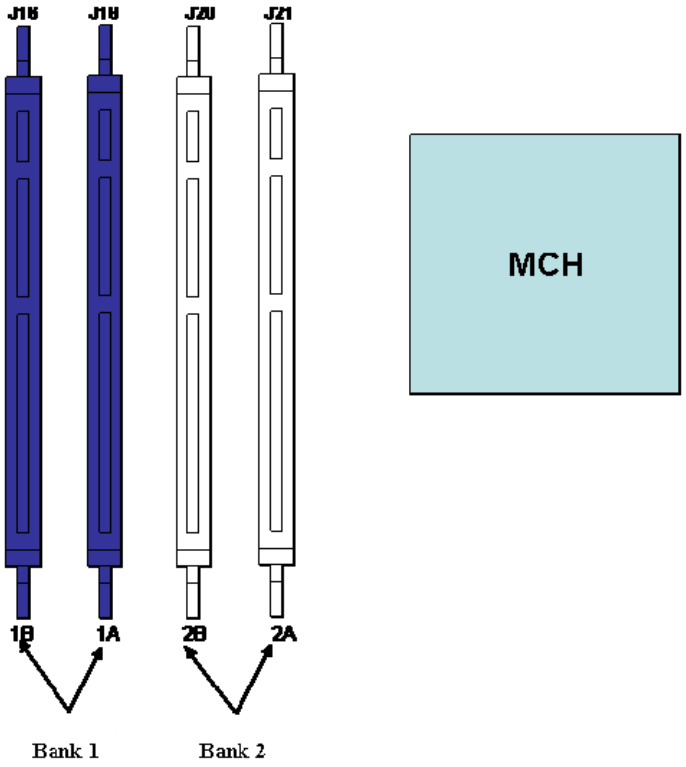


Figure 6. DIMM Socket Configuration

The following tables show supported memory populations. Table identifiers:

- S/R = single rank
- D/R = dual rank
- E = Empty

Table 4. Supported DDR-266 DIMM Populations

DIMM Slot A2	DIMM Slot A1	DIMM Slot B2	DIMM Slot B1
E	S/R	E	E
S/R	S/R	E	E
E	D/R	E	E
D/R	D/R	E	E
D/R	S/R	E	E

Table 5. Supported DDR-333 DIMM Populations

DIMM Slot A2	DIMM Slot A1	DIMM Slot B2	DIMM Slot B1
E	S/R	E	E
S/R	S/R	E	E
E	D/R	E	E
D/R	D/R	E	E
D/R	S/R	E	E

Table 6. DIMM Module Capacities

Parts	128Mb	256Mb	512Mb	1Gb
X8, single row		256 MB	512 MB	1 GB
X8, double row	256 MB	512 MB	1 GB	2 GB
X4, single row	256 MB	512 MB	1 GB	2 GB
X4, Stacked, double row	512 MB	1 GB	2 GB	4 GB

Table 7. Possible Memory Capacities

# of DIMMS	Spare	128 Mb	256 Mb	512 Mb	1 Gb
1		256 MB	512 MB	1 GB	2 GB
2	Single Channel	512 MB	1 GB	2 GB	4 GB
2		1 GB	2 GB	4 GB	8 GB
4	X	1 GB	2 GB	4 GB	8 GB
4	X	2 GB	4 GB	8 GB	

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

The minimum memory installed is 256 MB (one 256 MB DIMM).

3.5.3 I^2C Bus

To boot the system, the system BIOS uses a dedicated I^2C bus to retrieve DIMM information needed to program the MCH memory registers.

3.5.4 Disabling DIMMs

The BIOS provides a mechanism to disable a DIMM if it is detected to be faulty. A faulty DIMM is defined to have either multiple correctable errors or a single uncorrectable error on a single DIMM. Memory errors are logged during runtime and CMEs (Correctable Memory Error) are counted, the CMEs include both single bit correctable and other correctable memory errors. Though DIMMs are marked as disabled, they are actually disabled only during the next reboot.

At the next system boot, memory-sizing code reads the recorded state of the DIMMs and skips sizing DIMMs marked as disabled. Because DIMMs are always used in 2-way interleaving, the DIMM pair is disabled. The disabled DIMMs are indicated by an LED next to the DIMM socket. If all DIMMs in a system have been disabled, the BIOS generates beep codes to indicate that the system has no usable memory.

Disabled DIMMs/rows may be re-enabled through a BIOS Setup option (Advanced Menu | Memory Configuration Sub-menu | Memory Retest | change setting to “enabled” | Exit Menu | Save changes and Exit). The DIMM slot will no longer be disabled if the system boots without memory in the DIMM slot.

3.5.4.1 Mechanism for CME/SEC Counter

The expected error rates for DIMMs are stated per gigabyte of memory. This information comes from three sources:

- Intel experimental measurements (one and one-half errors per year)
- Data from a memory component vendor (one error per month)
- The results from a 10-year study by a major computer manufacturer (four errors per month)

Since the lowest error rate was gathered over a short time, and the highest error rate was gathered over a long time, these two numbers are not considered valid and are discarded. The middle error number is perceived as being a more accurate conservative estimate and is used to program the threshold registers for single-bit correctable memory errors or SECs.

The threshold number must be adjusted for geographical areas of increased occurrence of alpha particles, which will increase error rates. Geographical effects include high altitudes and radioactive mineral deposits. Studies have shown that single-bit error rates at altitudes over 10,000 feet are 14 times higher than error rates at sea level. The highest of the three quoted error rates included various geographical locations.

Table 8 shows the suggested SEC register threshold for various DIMM sizes. The values in the table include a minimal error residue at one times the expected average error rate. Halving the time or threshold would result in loss of error count resolution. One register is programmed for each DIMM slot.

Table 8. Suggested SEC Threashold Prescale Settings

DIMM Size	SPARECTL SEC Prescale Value	SPARECTL SEC Prescale Unit	Thresh_SEC Count on a per DIMM Basis
128 MB	128	7h = week	4
256 MB	64	7h = week	4
512 MB	32	7h = week	4
1 GB	16	7h = week	4
2 GB	8	7h = week	4
4 GB	4	7h = week	4

In both runtime mode and non-RAS mode, the chipset counter defines the number of CMEs that can occur on each individual DIMM. The counter for the DIMM is also dependent on the DIMM size. The table below shows the resulting threshold values based on the DIMM size.

Table 9. DIMM Threshold Values by DIMM Size

DIMM Size	Threshold Value
64 MB	4
128 MB	4
256 MB	4 x 2
512 MB	4 x 4
1 GB	4 x 8
2 GB	4 x 16
4 GB	4 x 32

Example:

If the DIMM in socket 1A 256 MB, its counter value is 08h. If the CME count that occurs on this DIMM is over 08h, then the DIMM 1A LED will be lit and the CME logging and detection will be disabled by BIOS.

If the DIMM in socket 2A is 512 MB, its counter value is 10h. If the CME count that occurs on this DIMM is over 10h, then the DIMM 2A LED will be lit and the CME logging and detection will be disabled by BIOS.

3.5.5 Memory RASUM Features

The Intel® E7320 MCH and Intel E7525 MCH support several memory RASUM (Reliability, Availability, Serviceability, Usability, and Manageability) features that have traditionally been found only on high end server systems. These features include x4 SDDC for memory error detection and correction, Memory Scrubbing, Retry on Correctable Errors, Integrated Memory Initialization, and DIMM Sparing. The following sections describe how each is supported on these server boards.

3.5.5.1 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. x4 SDDC ECC is not supported during single-channel operation outside of DIMM mirroring fail-down because it does have significant performance impacts in that environment.

3.5.5.2 Integrated Memory Scrub Engine

The Intel® E7320 and Intel E7525 MCHs include 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, an 8 GB system can be completely scrubbed in less than one day. (The effect of these 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.

3.5.5.3 Retry on Uncorrectable Error

The Intel® E7320 and Intel E7525 MCHs include 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 (statistically very unlikely). This RASUM feature may be enabled and disabled via configuration.

3.5.5.4 Integrated Memory Initialization Engine

The Intel® E7320 and Intel E7525 MCHs provide 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, and provides a BIOS-accessible memory zeroing capability for use by the operating system.

3.5.5.5 DIMM Sparing Function

To provide a more fault tolerant system, the Intel® E7320 MCH and Intel E7525 MCH include 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 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: *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: set the fail-over threshold register to a non-zero value to enable the feature, 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. (This

requires that the spare DIMM be at least the size of the largest primary DIMM in use.) 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.

This 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.

3.6 I/O Sub-System

The I/O sub-system is made up of several components: the MCH providing the PCI Express* interface and the Intel® 6300ESB I/O controller providing the interface for the onboard video controller, Super I/O chip, and Management Sub-system. This section describes the function of each I/O interface and how they operate on these server boards.

3.6.1 PCI Subsystem

The primary I/O interface is PCI, with two independent PCI bus segments. A PCI 33 MHz, 32-bit bus segment (P32-A) with two connectors and a PCI-X 64-bit / 66 MHz segment (P64-A) are controlled through the Intel® 6300ESB I/O controller. Additionally, one x4 PCI Express* (P64-Express4) bus segment controlled from the MCH on the Intel Server Board SE7320SP2 is available. Or one x4 PCI Express bus segment and one x16 PCI Express bus segment (P64-Express16) are available on the Intel Server Board SE7525GP2. The table below lists the characteristics of the different PCI bus segments.

Table 10. 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	2 slots
P64-A	3.3 V	64-bits	66 MHz	PCI-X	2 slots
P64-Express4	1.6 V	64-bits	x4	PCI-E	1 slot
P64-Express16	1.6 V	64-bits	x16	PCI-E	1 slot (SE7525GP2 only)

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

All 32-bit, 33-MHz PCI I/O is directed through the Intel® 6300ESB I/O controller. The 32-bit, 33-MHz PCI segment created by the Intel 6300ESB I/O controller is known as the P32-A segment. The P32-A segment supports the following devices:

- 2D/3D Graphics Accelerator: ATI* Rage XL video controller

- SIO Chip: National Semiconductor* PC87417 Super I/O
- Hardware monitoring sub-system: SMBUS
- Intel® 82541 PCI gigabit NIC
- Two expansion slots

3.6.1.2 P64-A: 64-bit, 66 MHz PCI Subsystem

One 64-bit PCI-X bus segment is directed through the Intel® 6300ESB I/O hub. The PCI-X segment, P64-A, supports the interface for two 3.3-V, 64-bit PCI-X slots.

3.6.1.3 P64-Express4: x4 PCI Express* Bus Segment

The P64-Express4 bus segment supports x4 PCI Express* signaling. These server boards implement a x8 PCI Express connector on this bus to enhance the breadth of supported devices, however all devices will operate at a maximum speed of x4 (2 GB/s).

3.6.1.4 P64-Express16: x16 PCI Express bus segment

Intel® Server Board SE7525GP2 only: The P64-Express16 bus segment supports x16 PCI Express signaling.

3.6.1.5 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 will be increased by one.

3.6.1.6 Resource Assignment

The resource manager assigns the PIC-mode interrupt for the devices that will be accessed by the legacy code. The BIOS will ensure the PCI BAR registers and the command register for all devices are correctly set up to match the behavior of the legacy BIOS. Code cannot make assumptions about the scan order of devices or the order in which resources will be allocated to them. The BIOS will support the INT 1Ah PCI BIOS interface calls.

3.6.1.7 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.

3.6.1.8 Option ROM Support

The option ROM support code in the BIOS will dispatch the option ROMs in available memory space in the address range 0c0000h-0e7fffh and will follow all rules with respect to the option ROM space. The BIOS integrates option ROMs for all the integrated components on the board.

3.6.1.9 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.

3.6.2 Split Option ROM

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

3.6.3 Interrupt Routing

The interrupt architecture accommodates both PC-compatible PIC mode and APIC mode interrupts through use of the integrated I/O APICs in the Intel 6300ESB I/O controller.

3.6.3.1 Legacy Interrupt Routing

For PC-compatible mode, the Intel 6300ESB I/O controller 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 Intel 6300ESB I/O controller contains configuration registers that define which interrupt source logically maps to I/O APIC INTx pins.

Interrupts, both PCI and IRQ types, are handled by the Intel 6300ESB I/O controller. The Intel 6300ESB I/O controller then translates these to the APIC bus. The numbers in the table below indicate the Intel 6300ESB I/O controller PCI interrupt input pin to which the associated device interrupt (INTA, INTB, INTC, INTD) is connected. The Intel 6300ESB I/O controller I/O APIC exists on the I/O APIC bus with the processors.

Table 11. PCI Interrupt Routing/Sharing

Interrupt	INT A	INT B	INT C	INT D
Video	PIRQB			
Intel® 82541 NIC	PIRQA			
PCI Slot 3 (PCI 32b/33M)	PIRQF	PIRQD	PIRQB	PIRQH
PCI Slot 5 (PCI 32b/33M)	PIRQE	PIRQB	PIRQH	PIRQD
PCI Slot 2 (64b/66M)	PXIRQ1	PXIRQ2	PXIRQ3	PXIRQ0
PCI Slot 1 (64b/66M)	PXIRQ0	PXIRQ1		

3.6.3.2 APIC Interrupt Routing

For APIC mode, 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.

3.6.3.3 Legacy Interrupt Sources

The table below recommends the logical interrupt mapping of interrupt sources. The actual interrupt map is defined using configuration registers in the Intel® 6300ESB I/O controller.

Table 12. Interrupt Definitions

ISA Interrupt	Description
INTR	Processor interrupt
NMI	NMI to processor
IRQ0	System timer
IRQ1	Keyboard interrupt
IRQ2	Slave PIC
IRQ3	Serial port 1 or 2 interrupt from SUPER I/O device, user-configurable
IRQ4	Serial port 1 or 2 interrupt from SUPER I/O device, user-configurable
IRQ5	Parallel Port / Generic
IRQ6	Floppy disk
IRQ7	Generic
IRQ8_L	Active low RTC interrupt
IRQ9	SCI*
IRQ10	Generic
IRQ11	Generic
IRQ12	Mouse interrupt
IRQ13	Floating point processor
IRQ14	Compatibility IDE interrupt from primary channel IDE devices 0 and 1
IRQ15	Secondary IDE cable
SMI*	System management interrupt. General purpose indicator sourced by the 6300ESB to the processors.

3.6.3.4 Serialized IRQ Support

The server boards support 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 the quiet mode may initiate the start frame. While in the continuous mode, the start frame is initiated by the host controller.

3.6.3.5 IRQ Scan for PCI IRQ

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 boards have an external PCI interrupt serializer for PCI IRQ scan mechanism of Intel 6300ESB I/O controller to support 16 PCI IRQs.

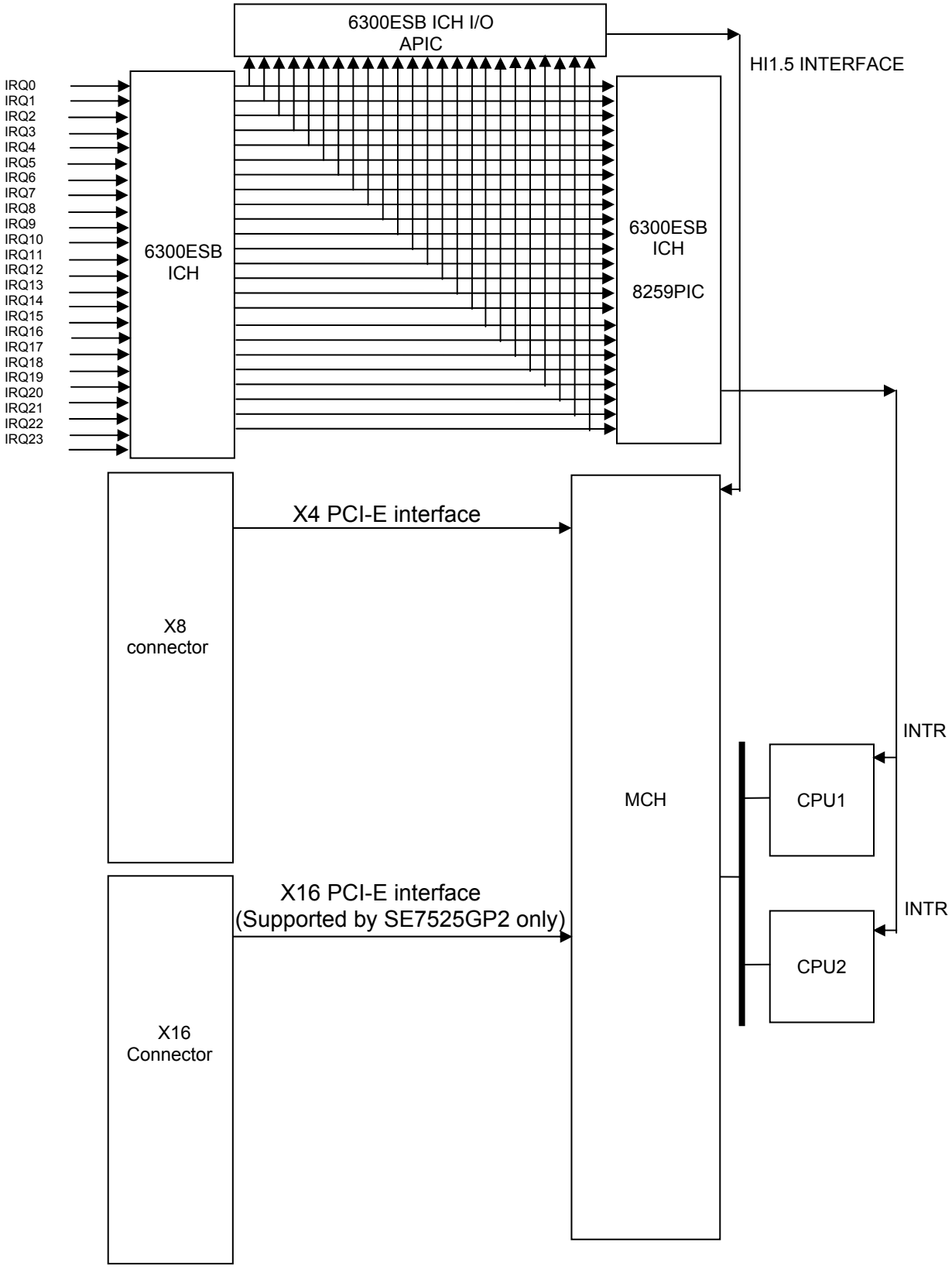


Figure 7. Interrupt Routing (Intel® 6300ESB Internal)

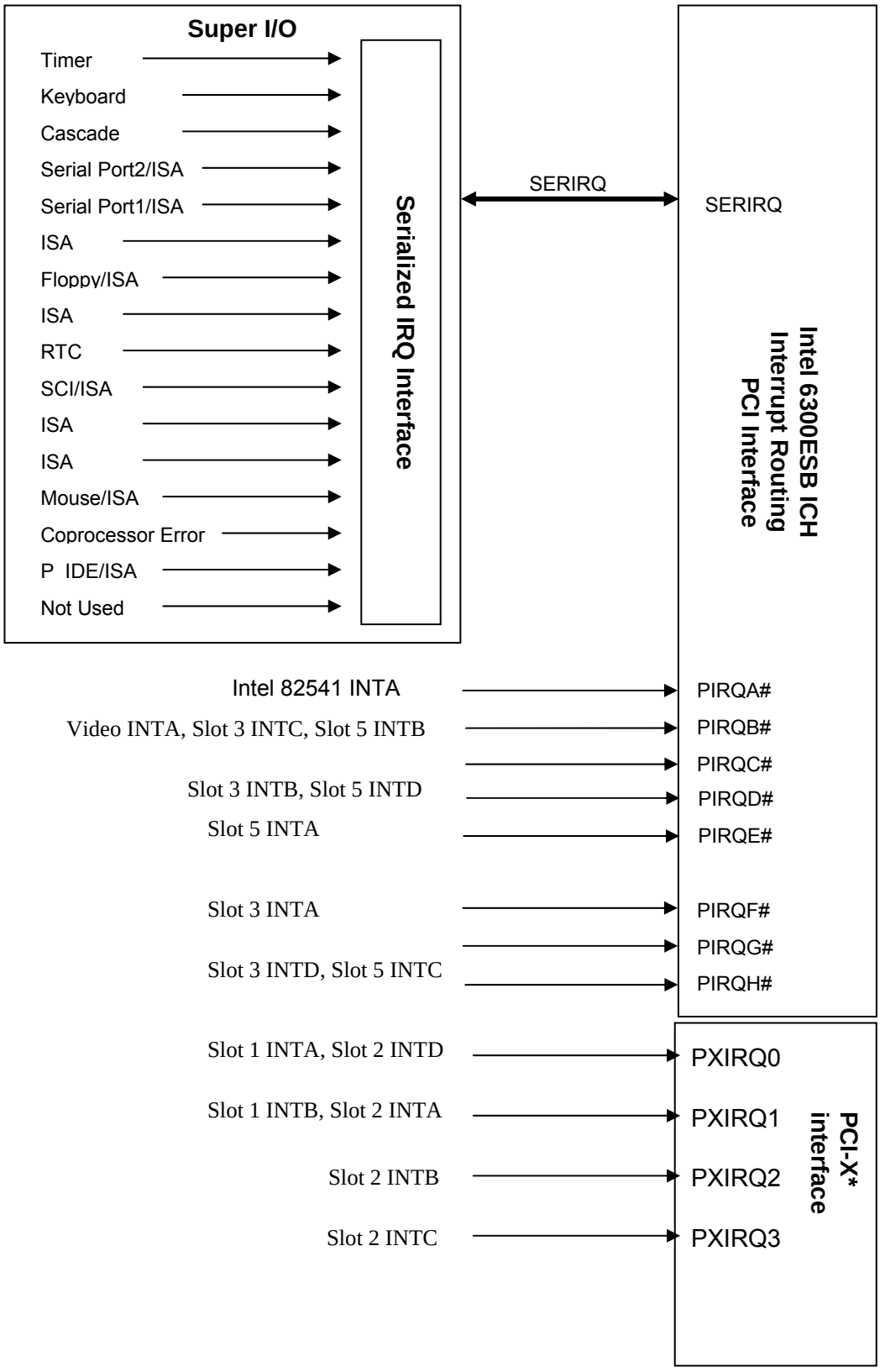


Figure 8. Interrupt Routing

3.6.4 IDE Support

Integrated IDE controllers of the Intel® 6300ESB I/O controller provide two independent IDE channels, each capable of supporting up to two drives. Both channels provide a standard 40-pin IDE connector on the server board. Each IDE channel can be configured or enabled/disabled by accessing the BIOS Setup Utility during POST.

3.6.4.1 Ultra ATA/100

The IDE interfaces of the Intel 6300ESB I/O controller DMA protocol redefines signals on the IDE cable to allow both host and target throttling of data and transfer rates of up to 100 MB/s.

3.6.4.2 IDE Initialization

The BIOS supports the ATA/ATAPI Specification, version 6 or later. The BIOS initializes the embedded IDE controller in the chipset (Intel 6300ESB I/O controller) 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 will 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.

3.6.5 SATA Support

The integrated Serial ATA (SATA) controller of the Intel 6300ESB I/O controller provides two SATA ports on the server board. The SATA ports can be enabled/disabled and/or configured by accessing the BIOS Setup Utility during POST.

The SATA function in the Intel 6300ESB I/O controller has dual modes of operation to support different operating system conditions. In the case of Native IDE enabled operating systems, the Intel 6300ESB I/O controller 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. Device 31, Function 1 (IDE controller) is hidden by software writing to the Function Disable Register (D31, F0, offset F2h, bit 1), 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 Intel® 6300ESB I/O controller 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 Intel 6300ESB I/O controller 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.

3.6.5.1 SATA RAID

The Intel® RAID Technology solution, available with the Intel 6300ESB I/O controller, offers data stripping for higher performance (RAID Level 0) or data mirroring for better data protection (RAID 1). There is no loss of PCI resources (request/grant pair) or add-in card slot.

Intel RAID Technology functionality requires the following items:

- Intel® 6300ESB
- 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 - D31:F0:AE bits [7:6] have been cleared

3.6.5.2 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.

3.6.6 Video Controller

Both server boards provide 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. Onboard video can be disabled using the BIOS Setup Utility which is accessed during POST or when an add-in video card is installed in any of the PCI slots.

3.6.6.1 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 13. 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**			
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**			
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	–	–

3.6.6.2 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 boards support an 8-MB (512 KB x 32-bit x four banks) SDRAM device for video memory. The following table shows the video memory interface signals:

Table 14. 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

3.6.7 Network Interface Controller (NIC)

3.6.7.1 Intel® 82541

The Intel® 82541 gigabit network interface controller supplies the server board with a single network interface. The 82541 controller is capable of supporting 10/100/1000 operation and alert-on-LAN functionality. The controller can be disabled by using the BIOS Setup Utility accessed during POST. The 82541 supports the following features:

- 32-bit PCI Rev. 2.3 compliant 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

3.6.7.2 NIC Connector and Status LEDs

The Intel® 82541 network controller drives two LEDs located on the 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 1000-Mbps operations when amber, 100-Mbps operations when green, and 10-Mbps when off.

3.6.8 USB 2.0 Support

The USB controller functionality integrated into Intel® 6300ESB I/O controller provides the server board with the interface for up to four USB 2.0 ports. Two external connectors are located on the back edge of the server board. One internal 2x5 header is provided which is capable of supporting an additional two optional connectors.

3.6.9 Super I/O Chip

The Server I/O is the National Semiconductor* PC87427 controller. It is located on the Intel® 6300ESB I/O controller LPC bus. For LPC and SMBus access, the PC87427features a fast X-Bus, over which boot flash and I/O devices can be accessed. The PC87427supports X-Bus address line forcing (to 0 or 1) to access two BIOS code and data sets. The SMBus also controls serial port float, RTC access, and serial port interconnection (snoop and take-over modes). The PC87427 system health support includes a serial interface to LMPC0 health sensors, fan monitoring and control, and a chassis intrusion detector. The PC87427 also incorporates a Floppy Disk controller (FDC), two serial ports (UARTs), a keyboard and mouse controller (KBC), General-Purpose I/O (GPIO), GPIO extension for additional off-chip GPIO ports, and an interrupt serializer for parallel IRQs.

PC87427 features:

- 3.3V operation, Standby powered.
- Legacy modules: FDC, two Serial ports (UARTs) and a keyboard and mouse controller (KBC).
- LPC interface
- 8/16-bit fast X-Bus extension for boot flash, memory and I/O.
- Two sets of BIOS code and data support, for main and back-up BIOS.
- System health support, including LMPC sensor interface, fan monitor/control, and chassis intrusion detection, for all configurations (i.e., with or without a BMC or mBMC).
- Serial Interface for manageability (Serial Interface M). Two-to-one internally multiplexing of Serial Ports 1 and 2.
- One external serial port
- One internal serial port
- 52 GPIO ports with a variety of wake-up events plus GPIO extension for additional off-chip GPIO ports.
- Watchdog for autonomous system recovery for BIOS Boot process and for operating system use.
- Pulse-Width-Modulated Fan Speed Control and Fan Tachometer Monitoring

3.6.9.1 GPIOs

The National Semiconductor* PC87427 Super I/O provides nine general-purpose input/output pins that the SE7320SP2 and Server Board SE7525GP2 utilizes. The following table identifies the pin and the signal name used in the schematic:

Table 15. Super I/O GPIO Usage Table

Pin Name	(Powe Well)	GPI / GPO / Function	Signal Name	Function Description
GPIO00	Standby	Input	MANUF_DET_N	Active Low when Manufacturing Mode Detect (J35)
GPIO05/LMPCIF2	Standby	Input/Output	SIO_TEMP_SENSOR	Single wire temp sensor from LM30.
GPIO6	Standby	Output	BIOS_SEL	Selects BIOS flash bank (A21 bit) for rolling BIOS feature.
GPIO7/HFCKOUT	Standby	Output	CLK_10M_MBMC	HFCKOUT- 10 MHz clock to mBMC (not used)
GPIO27/SUPER IOSMI	Standby	Output	SUPER IO_SMI_N	Active Low to generate a SMI to 6300ESB ICH
GPIOE40	Standby	Input	2U_RISER_DETECT	Riser card type detect – Pin B92 of PCI-X Slot 1.
GPIOE41	Standby	Input/Output	RISER_PRESENT2	Riser card type detect – Pin B93 of PCI-X Slot 1.
GPIOE42	Standby	Input/Output	PCIE_WAKE_N	Input- Wake up Event from PCI-E Bus
GPIOE43	Standby	Input/Output	PME_N	Intput- PME from PCI Bus
GPIOE44/SCI	Standby	Input/Output	SUPER IO_PME_N	Output- Active Low to generate a PME to the 6300ESB ICH
GPIOE45/LED	Standby	Input/Output	PME_PCIX_N	Input- PME from PCI-X Bus
GPIO50/DCDM_N	Standby	Input/Output	NWY_DIS_N	Output- Active Low to disable Intel® 82570EI
GPIO51/DSRM_N	Standby	Input/Output	KNI_DIS_N	Output – Active low to disable Kenai-II
GPIO52/CTSM/XCS1	Standby	Input/Output	FRU_LEDSEL_N	Output – FRU LED Selection
GPIO54/SINM	Standby	Input/Output	MROMB_PRESENT_N	Input- Active Low when ZCR card detect
GPO60/WDO_N	Standby	Output	MBMC_RST_BTN_N	Output- Active Low to reset system
GPO61/SMBSA	Standby	Output	SUPER IO_SMBUS_ADDR	SMBus slave address (SMBSA) select – pulled to ground with 10K resistor.
GPO62/LFCLK	Standby	Output	TP_SIO_45	Unused
GPEXC/GPIO56	Standby	Output	SUPER IO_SERIAL_CLK1	Output- Serial Clock to Port 80 circuit
GPEXD/GPIO57	Standby	Input/Output	SUPER IO_SERIAL_DAT	Output- Serial data to Port 80 circuit/FRU LED circuit
GPEXC2 / LMPCLK	Standby	Output	SUPER IO_SERIAL_CLK2	Output- Serial Clock to FRU LED circuit
LED1	Standby	Output	FP_PWR_LED_N	Output- Power LED

3.6.9.2 Serial Ports

Both the SE7320SP2 and Server Board SE7525GP2 provide two serial ports: an external DB9 Serial port, and an internal DH-10 Serial header. The following sub-sections provide details on the use of the serial ports.

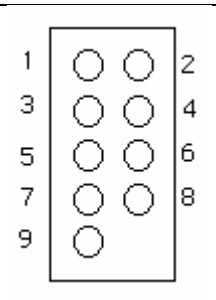
- **Serial Port A**

  Serial A is an external 9-pin DB-9 connector that is located on the back edge of the server board.

- **Serial Port B**

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

Table 16. Serial B 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	

3.6.9.3 Floppy Disk Controller

The 34-pin 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.

3.6.9.4 Keyboard and Mouse

Dual stacked PS/2 ports, located on the back edge of the server board, are provided for keyboard and mouse support. Either port can support a mouse or keyboard. Neither port supports “hot plugging” or connector insertion while the system is turned on.

3.6.9.5 Wake-up Control

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

3.6.10 BIOS Flash

An Intel® 3-volt Advanced+ Boot Block 28F320C3 Flash memory component is used as the BIOS flash device. The 28F320C3 is a high-performance 32-megabit memory component that provides 2048 K x 16 (4 MB) of BIOS and non-volatile storage space. The flash device is connected through the X-bus from the SIO.

3.7 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.

3.7.1 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 sub-regions as described in following sections. Attributes can be independently assigned to regions and sub-regions using the server board registers. The Intel® E7320 and Intel® E7525 chipsets each supports 64 GB of host-addressable memory space and 64 KB+3 of host-addressable I/O space. The server boards support up to 8 GB of main memory for DDR-266 or DDR-333 configurations.

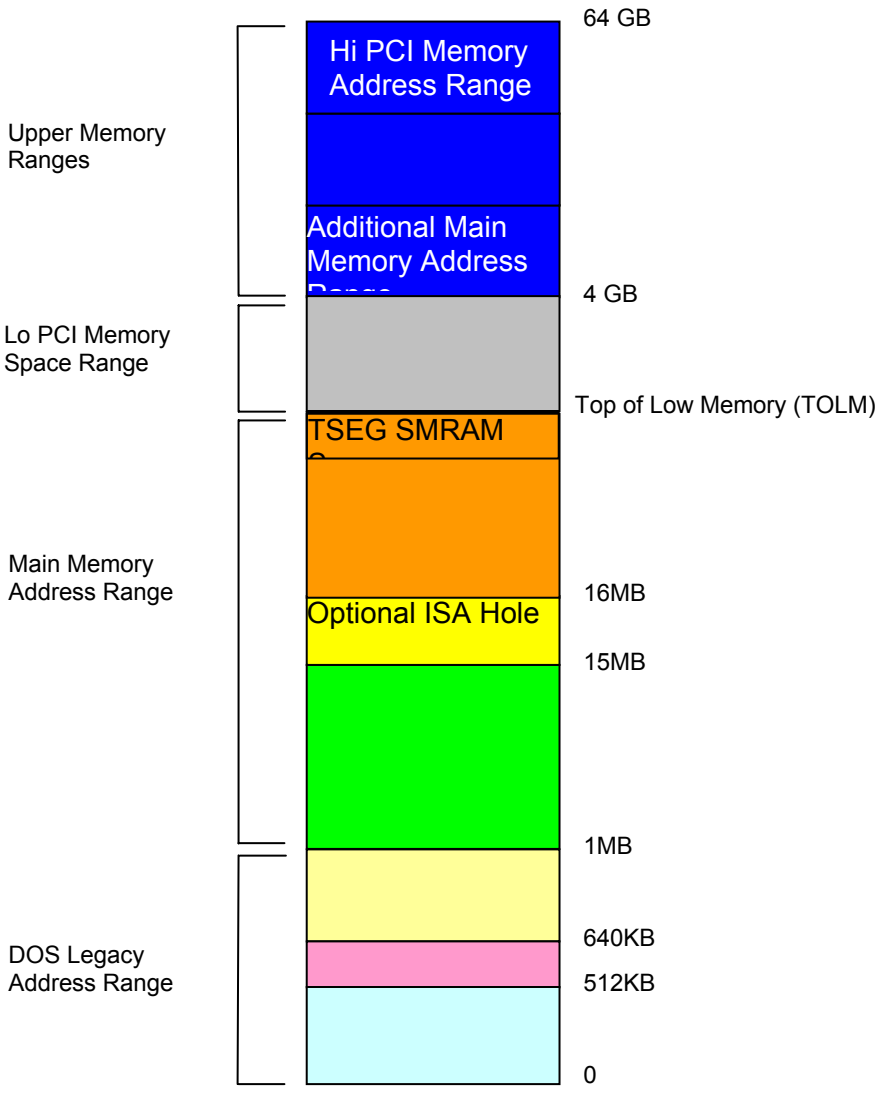


Figure 9. Intel® Xeon® Processor Memory address Space

3.7.1.1 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.

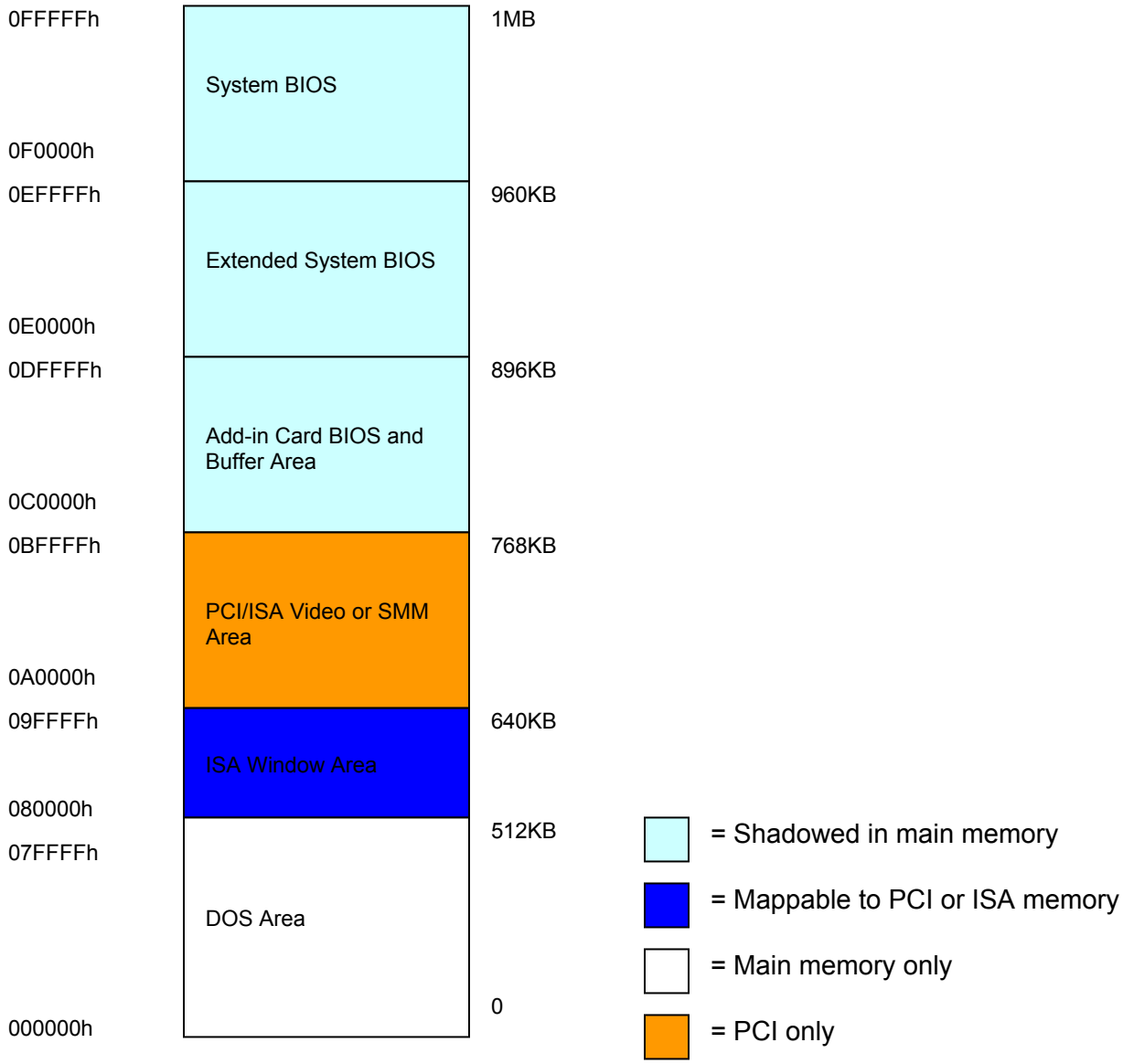


Figure 10. DOS Compatibility Region

- **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.

- **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.

- **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.

- **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.

- **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.

- **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.

3.7.1.2 Extended Memory

Extended memory is defined as all address space greater than 1 MB. Extended Memory region covers 8 GB 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).

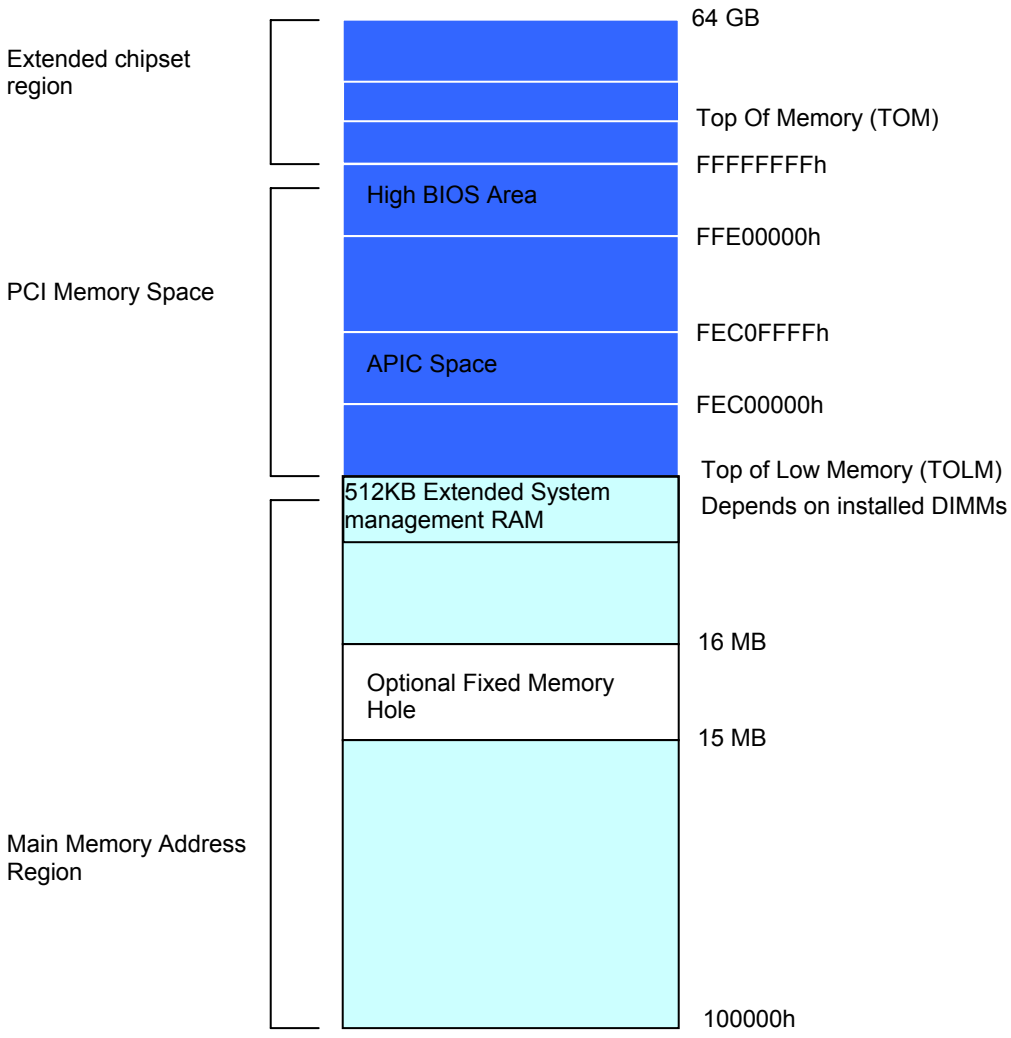


Figure 11 Extended Memory Map

- **Main Memory**

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

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

- **PCI Memory Space**

  Memory addresses below 4 GB 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.

- **High BIOS**

  The top 1 MB of Extended Memory under 4 GB 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.

- **I/O APIC Configuration Space**

  A 64 KB block located 20 MB below 4 GB (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.

- **Extended Intel® Xeon® Processor Region (above 4 GB)**

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

3.7.1.3 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.

3.7.1.4 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 which can be configured using the Intel 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

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

TSEG SMM is different than in previous chipset. In previous chipsets the TSEG address space was offset by 256 MB 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 256 MB and it is not remapped.

Table 17. 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

3.7.2 I/O Map

The server board I/O addresses to be mapped to the processor bus or through designated bridges in a multi-bridge system. Other PCI devices, including the Intel® 6300ESB I/O controller, have built-in features that support PC-compatible I/O devices and functions, which are mapped to specific addresses in I/O space. On SE7320SP2 and SE7525GP2, the Intel 6300ESB I/O controller 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 18. 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

Address (es)	Resource	Notes
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
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	

Address (es)	Resource	Notes
03E8h – 03Efh	Serial Port A	
03F0h – 03F5h	Floppy Disk Controller	
03F6h – 03F7h	Primary IDE – Sec Floppy	
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 SE7320SP2 Turbo and Reset Control	
0CFCh	PCI CONFIG_DATA Register	

3.7.3 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 should 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.

3.7.3.1 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 [8::2] select a specific register in the configuration space of the selected device or function on the bus.

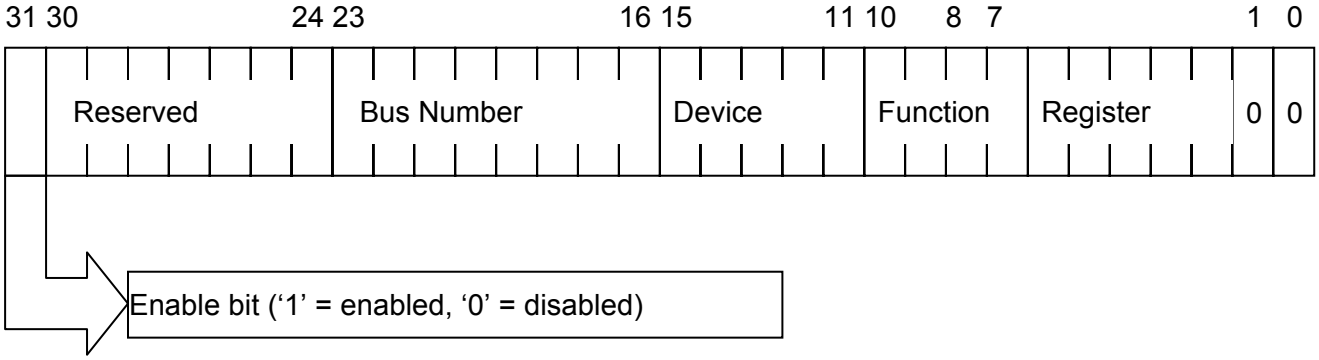


Figure 12. CONFIG_ADDRES Register

3.7.3.1.1 Bus Number

PCI configuration space protocol requires that all PCI buses in a system be assigned a Bus Number, Furthermore, 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.

3.7.3.1.2 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 5-bits of the device number are used in CONFIG_ADDRESS bits [15::11].

Table 19. 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

PCI Device	IDSEL	Bus# / Device# / Function#
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-D Slot1	P2A_AD17	/ 01 /
FL PXH-D Slot 2	P2B_AD17	/ 01 /
FL PCI-E x4 Slot1		/ ?? /
FL PCI-E x4 Slot2		/ ?? /
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 /
LP PCI-E x8 Slot1		/ ?? /
Onboard device		
Intel® 82546GB (1Gb) NIC with dual-channel	P1B_AD20	/ 04 / 0,1
LSI 53C1030 Ultra 320 SCSI with dual-channel	P1A_AD21	/ 05 / 0,1
ATI Rage XL (PCI VGA)	PC_AD28	/ 12 / 0

3.8 Clock Generation and Distribution

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

- 200 MHz differential Clock at 0.7 V logic levels. For Processor 0, Processor 1, Debug Port and MCH.
- 100 MHz differential Clock at 0.7 V logic levels on CK409B. For DB800 clock buffer.
- 100 MHz differential Clock at 0.7 V logic levels on DB800. For PCI Express* Device is MCH. And for SATA is Intel® 6300ESB.
- 66 MHz at 3.3 V logic levels: For MCH and Intel 6300ESB
- 48 MHz at 3.3V logic levels: For Intel 6300ESB and SIO.
- 33 MHz at 3.3V logic levels: For Intel 6300ESB, Video, BMC and SIO.
- 14.318 MHz at 2.5 V logic levels: For Intel 6300ESB and video.
- 10 MHz at 5V logic levels: For mini BMC.

3.8.1 Real Time Clock

The real time clock is specified to operate within the following criteria and environmental conditions:

- RTC accuracy: 1 minute per month = 2 seconds per day
- Environmental conditions:
  - Temperature: 10 ~ 35 C
  - Humidity: 20 ~80% (non-condensing)

4. System BIOS

This section describes the functionality and features supported of the system Basic Input/Output System (BIOS), which is based on an AMI 8.0 core architecture. The BIOS is implemented as firmware that resides in 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 embedded PCI devices.

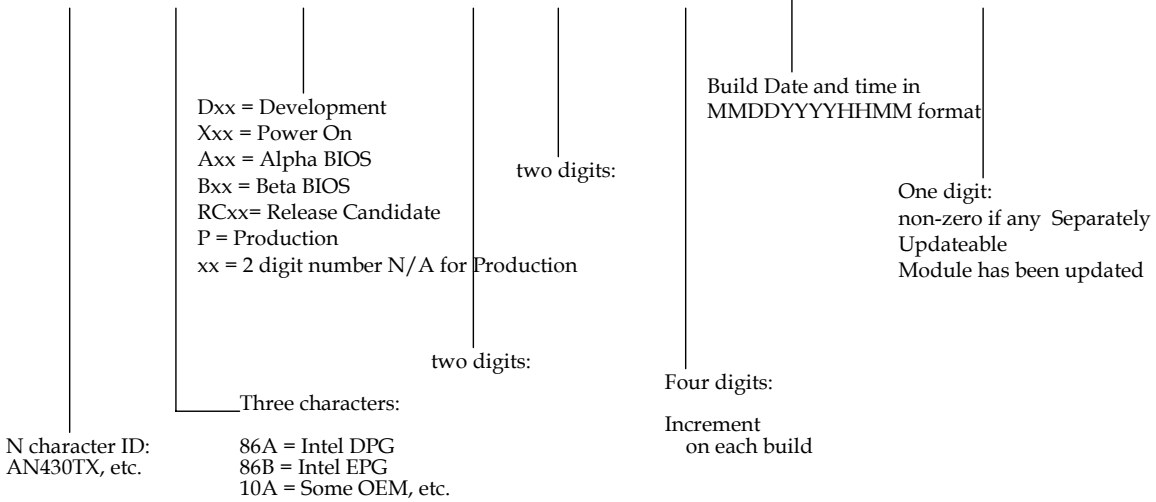
The BIOS is comprised of the following components:

- IA-32 core BIOS. This component contains most of the standard services and components found in an IA-32 system, such as the PCI Resource manager, ACPI support, POST, and RUNTIME functionality.
- The "EFI" is the extensible firmware interface. This is an abstraction layer between the operating system and system hardware.
- Server BIOS extensions: Support for Baseboard Management controller (BMC) and Intelligent Platform Management Interface (IPMI).
- Processor Microcode Updates: The BIOS also includes latest processor microcode updates.

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 follows:

BoardId.OEMID.BuildType.Major.Minor.BuildID.BuildDateTime.Mod



During board development, the system BIOS will have a unique BIOS ID for the sever boards. The following is a sample data string that will be displayed during POST:

```
SE7320SP2.86B.P.05.00.0028.10072004
SE7525GP2.86B.P.05.00.0028.10072004
```

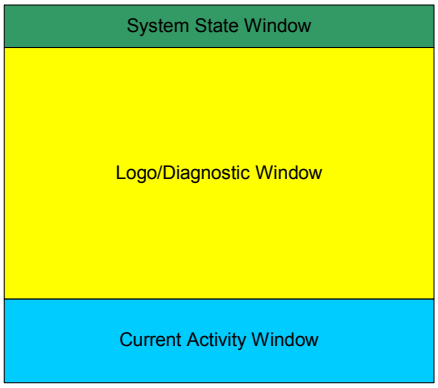
4.2 BIOS POST Splash Screen

The BIOS supports one system splash screen. When the system is booting, the BIOS will display the splash screen instead of BIOS messages. BIOS messages can be viewed by pressing the 'ESC' key during POST. Once the BIOS POST message screen is selected, the splash screen is no longer accessible during the current boot sequence. The splash screen can be customized by with the 'Change Logo' utility. Refer to the *Change Logo for AMIBIOS User's Guide* (Version 2.22) for details.

4.2.1 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 areas: the System Activity/State, Logo/Diagnostic, and Current Activity windows. The System Activity Window displays information about the current state of the system. The Logo/Diagnostic Window displays the OEM splash screen logo or a diagnostic boot screen. The Current Activity Window displays information about the currently executing portion of POST as well as user prompts and status messages.



4.2.1.1 System State 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.

4.2.1.2 Logo/Diagnostic Window

The middle portion of the screen is reserved for the Logo/Diagnostic Window. On a graphics console, the window is 640x384. On a text console, the window is 80x20.

The Logo/Diagnostic Window may be in one of two forms depending on whether Quiet Boot Mode is selected in the BIOS Setup. If selected, the BIOS displays a logo splash screen. If not, the BIOS displays a system summary and diagnostic screen in verbose mode. The default is to display the logo in Quiet Boot mode. If no logo is present in the flash ROM, or Quiet Boot mode is disabled in the system configuration, the summary and diagnostic screen is displayed. If the user presses <Esc>, the system transfers from the logo screen to the diagnostic screen.

4.2.1.3 Current Activity Window

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

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

4.2.1.4 System Diagnostic Screen

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

4.2.1.5 Static Information Display

The Static Information Display area presents the following information:

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

4.2.1.5.1 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 clearing 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.

4.2.1.5.2 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 20. 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

4.3 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 when prompted during POST by using the F2 key.

4.3.1 Localization

The BIOS Setup utility uses the Unicode standard and is capable of displaying setup forms in (EFIGS) languages currently included in the Unicode standard. The BIOS supports English, Spanish, French, German, and Italian. Intel provides translations for console strings in the supported languages. The language can be selected using BIOS user interface.

4.3.2 Console Redirection

The BIOS Setup utility is functional via console redirection over various terminal standards emulation. This may limit some functionality for compatibility, e.g., usage of colors or some keys or key sequences or support of pointing devices.

4.3.3 Configuration Reset

Setting the Clear CMOS jumper (board location J17) produces a “reset system configuration” request. When a request is detected, the BIOS loads the default system configuration values during the next POST.

Alternatively, the user can clear CMOS 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 and then release both simultaneously.

4.3.4 Keyboard Commands

The Keyboard Command Bar supports the following:

Table 21. BIOS Setup Keyboard Command Bar Options

Key	Option	Description
Enter	Execute Command	The Enter key is used to activate sub-menus when the selected feature is a sub-menu, or to display a pick list if a selected option has a value field, or to select a sub-field for multi-valued features like time and date. If a pick list is displayed, the Enter key will undo the pick list, and allow another 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.
	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 Optional 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 BIOS setup without affecting any existing field values
F10	Save 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 BIOS setup without affecting any existing values.

4.4 Entering BIOS Setup

The BIOS Setup utility is accessed by pressing the <F2> hot-key during POST.

Note: *Some BIOS setup options are based on latest BIOS. If your server has an older BIOS, you may see some differences.*

4.4.1 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 in **bold** text.

Table 22. BIOS Setup, Main Menu Options

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
Server Board MCH Stepping			
Stepping	N/A	N/A	Stepping of the MCH component
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.

4.4.2 Advanced Menu

Table 23. 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.

4.4.2.1 Processor Configuration Sub-menu

Table 24. 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.

Feature	Options	Help Text	Description
Cache L3	N/A	N/A	Displays cache L3 size. Visible only if the processor contains an L3 cache.
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.
HT Technology in MPS	**Disabled** Enabled	Enabling adds secondary processor threads to the MPS Table for pre-ACPI OSes. Only enable this feature if the pre-ACPI OS supports Hyper-Threading Technology	
Intel® SpeedStep™ Tech.	**Disabled** Auto	Select disabled for maximum CPU speed. Select enabled to allow the OS to reduce power consumption.	Visible only if the processor has this feature.
Execute Disable Bit	**Disabled** Enabled	Intel's Execute Disable Bit functionality can prevent certain virus attacks	Visible only if the processor has this feature.
Hardware Prefetcher	**Disabled** Enabled	This should be enabled in order to enable or disable the Hardware Prefetcher Disable feature	
Adjacent Cache Line Prefetch	**Disabled** Enabled	This should be enabled in order to enable or disable the Adjacent Cache Line Prefetch Disable Feature	

4.4.2.2 IDE Configuration Sub-menu

Table 25. BIOS Setup IDE Configuration Menu Options

Feature	Options	Help Text	Description
IDE Configuration			
Onboard PATA Channels	Disabled Primary Secondary **Both**	Disabled: disables the integrated PATA controller. Primary: enables only the Primary PATA controller. Secondary: enables only the Secondary PATA controller. Both: enables both PATA controllers.	Controls state of integrated PATA controller.
Onboard SATA Channels	Disabled **Enabled**	Disabled: disables the integrated SATA controller. Enabled: enables the integrated SATA controller.	Controls state of integrated SATA controller.
Configure SATA as RAID	**Disabled** Enabled	When enabled the SATA channels are reserved to be used as RAID.	
SATA Ports Definition	**A1-3rd M/A2-4th M** A1-4th M/A2-3rd M	Defines priority between SATA channels.	Default set the SATA Port0 to third IDE Master channel & Port1 to fourth IDE Master channel. Otherwise set SATA Port0 to fourth IDE Master channel and Port1 to third IDE Master channel.
Mixed PATA / SATA	N/A	Lets you remove a PATA and replace it by SATA in a given channel. Only 1 channel can be SATA.	Selects submenu for configuring mixed PATA and SATA.
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 80-pin ATA (PI) cable.	The 80-pin cable is required for UDMA-66 and above. The BIOS detects the cable by querying the host and/or device.

Table 26. Mixed PATA-SATA Configuration with only Primary PATA

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

Table 27. 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 asynchronous 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 is correct 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 is correct 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 is correct in most cases.
PIO Mode	**Auto** 0 1 2 3 4	Select PIO Mode.	The auto setting is correct 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 is correct in most cases.
S.M.A.R.T.	**Auto** Disabled Enabled	Self-Monitoring, analysis and reporting technology.	The auto setting is correct in most cases.
32Bit Data Transfer	**Disabled** Enabled	Enable / disable 32-bit data transfer	

4.4.2.3 Floppy Configuration Sub-menu

Table 28. 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 720 KB or 2.88 MB drives.
Onboard Floppy Controller	Disabled **Enabled**	Allows BIOS to enable or disable floppy controller.	

4.4.2.4 Super I/O Configuration Sub-menu

Table 29. BIOS Setup, Super I/O Configuration Sub-menu

Feature	Options	Help Text	Description
Configure National Semiconductor 42x Super I/O 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.

4.4.2.5 USB Configuration Sub-menu

Table 30. 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 unavailable.
Legacy USB Support	Disabled Keyboard only **Auto** Keyboard and Mouse	Enables support for legacy USB. Auto disables legacy support if no USB devices are connected. If disabled, USB Legacy Support will not be disabled until booting an operating system.	
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 operating systems.	
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.

4.4.2.6 USB Mass Storage Device Configuration Sub-menu

Table 31. 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 530 MB 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).	
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 530 MB 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).	

4.4.2.7 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 32. BIOS Setup, PCI Configuration Sub-menu Selections

Feature	Options	Help Text	Description
PCI Configuration			
Onboard Video	Disabled **Enabled**	Enable / disable onboard VGA controller	
Dual Monitor Video	**Disabled** Enabled	Select which graphics controller to use as the primary boot device. Enabled selects the onboard 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.
MMIO above 4 GB	**Disabled** Enabled	Enable / disable memory mapped I/O of 64-bit PCI devices to 4 GB or greater address space	
MMIO below PCI Express MMCFG	**Enabled** Disabled	Disabled: Highest PCI address set just below 4 GB for memory allocation, but not compatible for all configurations with a PCI bridge aperture that spans PCI Express MMCFG space (3.5-3.75 GB). Enabled: Highest PCI address set to 3.5 GB, just below PCI Express MMCFG	
Slot 1 Option ROM	Disabled **Enabled**	Full-height PCI-X 64/66	Available only when PCI card installed.
Slot 2 Option ROM	Disabled **Enabled**	Full-height PCI-X 64/66	Available only when PCI card installed.
Slot 3 Option ROM	Disabled **Enabled**	Full-height PCI 32/33	Available only when PCI card installed.
Slot 4 Option ROM	Disabled **Enabled**	Full-height PCI Express* X4	Available only when PCI card installed.
Slot 5 Option ROM	Disabled **Enabled**	Full-height PCI 32/33	Available only when PCI card installed.
Slot 6 Option ROM	Disabled **Enabled**	Full-height PCI Express X16	Available only when PCI card installed. Not visible on the SE7320SP2 SKU.

4.4.2.8 Memory Configuration Sub-menu

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

Table 33. BIOS Setup, Memory Configuration Sub-menu Selections

Feature	Options	Help Text	Description
System Memory Settings			
DIMM 1A	Installed Not Installed Disabled Spare		Informational display.
DIMM 1B	Installed Not Installed Disabled Spare		Informational display.
DIMM 2A	Installed Not Installed Disabled Spare		Informational display.
DIMM 2B	Installed Not Installed Disabled 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 automatically 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 Sparing	**Disabled** Spare	Disabled provides the most memory space. Sparing reserves memory to replace failures.	Grayed out if the installed DIMM configuration does not support it.

4.4.3 Boot Menu

Table 34. 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.

4.4.3.1 Boot Settings Configuration Sub-menu Selections

Table 35. 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**	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.	

4.4.3.2 Boot Device Priority Sub-menu Selections

Table 36. 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.	

Note: *The boot sequence will be reset by the BIOS whenever a controller card that is listed in the boot menu is changed or removed. Return to this menu any time a configuration change is made to a bootable controller card.*

4.4.3.2.1 Hard Disk Drive Sub-menu Selections

Table 37. 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.

4.4.3.2.2 Removable Drive Sub-menu Selections

Table 38. 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.

4.4.3.2.3 ATAPI CD-ROM Drives Sub-menu Selections

Table 39. 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.

4.4.4 Security Menu

Table 40. 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**	No access: prevents User access to the Setup Utility. View Only: allows access to the Setup Utility but the fields can not be changed. Limited: allows only limited fields to be changed such as date and time. Full Access: 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.
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.
Front Panel Switch Inhibit	**Disabled** Enabled	When disabled, allows the use of Front Panel Switch. When enabled, inhibits Power Switch and Reset Switch button. Disables the Power Switch and the Reset Switch when Secure mode is activated.	This node is grayed out if a password is not installed or if the AC Policy is set to “Stays Off.”
NMI Control	**Disabled** Enabled	Enable / disable NMI control for the front panel NMI button.	

4.4.5 Server Menu

Table 41. BIOS Setup, Server Menu Selections

Feature	Options	Help Text	Description
System management	N/A	N/A	Selects submenu.
Power Management Features	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.

Feature	Options	Help Text	Description
Resume on AC Power Loss	**Stays Off** Power On	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.	When set to “Stays Off,” “Front Panel Switch Inhibit” is disabled.
FRB-2 Policy	**Retry on Next Boot** Disable FRB2 Timer	This controls action if the boot processor will be disabled or not.	
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.	

4.4.5.1 System Management Sub-menu Selections

Table 42. BIOS Setup, System Management Sub-menu Selections

Feature	Options	Help Text	Description
System Management			
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
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

4.4.5.2 Power Management Features Sub-menu Selections

Feature	Options	Help Text	Description
Power Management Features			
Wake On LAN	**Disabled** Enabled	Enable / disable LAN GPI or PME to generate a wake event	

4.4.5.3 Serial Console Features Sub-menu Selections

Table 43. 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.	
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.	

4.4.5.4 Event Log Configuration Sub-menu Selections

Table 44. 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.	Option will be automatically set back to Disabled at the next reboot.
Clear Event Log When Full	**Disabled** Enabled	If enabled, BIOS will clear system event log upon system boot when it is full	
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.
Timestamp Clock Sync. event	**Enabled** Disabled	Enables or disables logging of the timestamp clock synchronization. Event for mBMC clock synchronization with RTC	

4.4.6 Exit Menu

Table 45. 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 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.

The complete ROM is visible, starting at physical address 4 GB minus the size of the flash ROM device. The Flash Memory Update utility loads the BIOS image minus the recovery block to the secondary flash partition, and notifies the BIOS that this image should be used on the next system re-boot. Because of shadowing, none of the flash blocks are visible at the aliased addresses below 1 MB.

A 16 KB parameter block in the flash ROM is dedicated to storing configuration data that controls the system configuration (ESCD). Application software must use standard APIs to access these areas; application software cannot access the data directly.

4.6 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 is 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 first 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 “rollback”.

If a user wishes to force the system to boot to the primary bank, the jumper at J29 can be used. In the default jumper position with pins 1-2 covered, the rolling BIOS configuration is automatic. If the jumper is moved to cover pins 2-3, then the system will boot to the primary bank every time.

The rolling one-boot update feature applies to all the update mechanisms discussed in the following sections.

4.7 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.

4.7.1 Flash BIOS

The BIOS flash utility is compatible with DOS, Microsoft* Windows* 2000/2003/XP, Linux and EFI operating environments.

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

The format and usage of the afuXXX utility is as follows:

```
afuXXX /i<ROM filename> [/n] [/p[b][n][c]] [/r<registry_path>]
[/s] [/k] [/q] [/h]
```

Where:

- /n don't check ROM ID
- Choose one:
  - /pb Program Boot Block
  - /pn Program NVRAM
  - /pc Destroy System CMOS
- /r registry path to store result of operation (only for Windows version)
- /k Program non-critical block only
- /s Leave signature in BIOS
- /q Silent execution
- /h Print help

4.7.1.1 Updating the BIOS from DOS

- Make sure that the flash bootable disk contains both the ROM image and the afudos update utility.
- Boot to DOS.
- Run the afudos utility as follows:

```
AFUDOS /i<ROM filename> [/n][/p[b][n][c]]
```

4.7.1.2 Updating the BIOS from Microsoft* Windows* 2000/2003/XP

- Make sure that the flash disk contains the ROM image, AMIFLDRV.SYS and AFUWIN.EXE.
- Boot to Microsoft Windows 2000/2003/XP.
- Run the AFUWIN utility as follows:

```
AFUWIN /i<ROM filename> [/n][/p[b][n][c]]
```

4.7.1.3 Updating the BIOS from Linux

- Make sure that the flash disk contains the ROM image and the AFULNX utility.
- Boot to Linux and set up a floppy device.
- Run the AFULNX utility as follows:

```
./afulnx /i<ROM filename> [/n][/p[b][n][c]]
```

4.7.1.4 Updating the BIOS from the EFI Shell

- Make sure that the flash disk contains the ROM image and the AFUEFI utility.
- Boot to the EFI Shell with the flash disk.
- Do a map -r to retrieve the file system on the disk.
- Change to the flash disk, e.g., if the flash disk is fs0:, type fs0: at the prompt.
- Run the afuefi utility as follows:

  `afuefi [/n] [/p[b][n][c]] <ROM filename>`

4.7.2 User Binary Area

The server board 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.

The command line usage for the UbinD utility is as follows:

```
UBinD </R> or </I> or </D> [/M<ModID>] /F<RomFileName>
/B<NewUserBinaryFileName> [/N<NewRomFileName>] [/O<NCB>]
```

Where:

- `</R>` replaces the user binary module
- `</I>` inserts the user binary module
- `</D>` deletes the user binary module from the ROM file.
- `</?>` displays help information.
- `/M<ModID>` is hexadecimal user binary module ID; Default ModID = 0xF0.
- `/O<NCB>` is the 0-based index of the non-critical block number calculated from the start of the ROM file. Default NCB = 1, used only with the insert option. See ROMInfo for reference.
- `</N<NewRomFileName>` if this option is not included, the ROM is saved with the same name.

4.7.3 Recovery Mode

Three conditions can cause the system to enter recovery mode:

- Pressing a hot key
- Setting the recovery jumper (J17, 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.

4.7.3.1 BIOS Recovery

The BIOS has a ROM image size of 2 MB. A standard 1.44 MB 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 recover (see Section 4.7.3.2 for further details).

The BIOS contains a primary and secondary partition, and can support rolling BIOS updates (see Section 4.6 for details). 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, or an ATAPI CD-ROM/DVD.

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

The recovery mode procedure is as follows:

- Insert or plug-in the recovery media with the AMIBOOT.ROM file.
- 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).
- When F3 is displayed on port 80h, the system will read the BIOS image file.
- The screen will display flash progress and indicate whether the NVRAM and CMOS have been destroyed.
- When recovery mode is complete, the system will halt and the system can be powered off.

***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.

4.7.3.2 Multi-disk Recovery

The Multi-disk Recovery method is available to support ROM images greater than 1 MB when performing a BIOS recovery from multiple floppy disks.

Do the following to perform a multi-disk BIOS recovery:

1. Use the SPLIT.EXE utility to split the ROM image.

2. Execute the following command at the command prompt:

   `split <File Name To Be Split> <New File Name> <File Size in KB>`
   Example: `C:\split AMIBOOT.ROM AMIBOOT 1024`

   This command creates files of size 1 MB each (1024 KB) with the names AMIBOOT.000, AMIBOOT.001... and so on. The number of files (or floppy disks) depends upon the size of the AMIBOOT.ROM file.

3. Load the first disk with the AMIBOOT.000 file into the system.

   After reading the file, the system will increment the file extension and begin searching for the second file, AMIBOOT.001, on the same floppy disk.

4. If the system cannot find the file on the floppy disk, it beeps once for one second, and then searches again. After the beep, load the second floppy disk.

The system will continue reading and searching for files. Once a file has been read, the system will increment the file extension and then begin searching for the next file. If searching for the AMIBOOT.002 file, the system will beep twice, each beep for one second, with a 0.5 second gap between beeps. If searching for the AMIBOOT.003 file, the system will beep three times with a 0.5 sec gap between beeps.

This process would continue until the total file size read in is equal to the size of the ROM image.

Limitation:

The maximum number of files supported by the multi-disk recovery method is 1,000 files (AMIBOOT.000 through AMIBOOT.999).

4.7.4 Update OEM Logo

The OEM logo can be changed in the BIOS for DOS and Microsoft Windows* 2000 / 2003 / XP. A utility tool is used to change the OEM logo in ROM. The OEM logo can then be updated by flashing the ROM.

For details on how to replace the logo with an OEM logo, download and follow the instructions in *Customize BIOS with OEM Logo* white paper available on the Intel Support website.

Command-line Usage:

```
OEMLogo <RomFileName> <NewOEMImageFileName> [/F or /FN or /N]
```

or

```
OEMLogo <RomFileName> [/D]
```

Where

- `[/F]` forces replacement of the OEM logo even if the logo formats do not match.
- `[/N]` inserts the 16-color BMP without converting it to the default AMI format.
- `[/FN]` forces replacement of the OEM logo without converting a 16-color BMP to the default AMI format.
- `[/D]` deletes the logo module from the ROM file.

Supported formats are dependent on the ROM and include the following:

- 16-color BMP, size up to 640x480, even width
- 256-color BMP, 640x480
- JPEG, 640x480, 800x600, or 1024x768
- 256-color PCX, 640x480

***Note**: The Rombuild.exe file is NOT the same for DOS and Microsoft Windows 2000 / 2003 / XP. The user must use the correct Rombuild.exe file for the operating system.*

4.7.4.1 Changing the OEM Logo for DOS

1. Boot to DOS.
2. Download OEMLOGOD.exe, Rombuild.exe, RomFile, and NewOEMlogoImage to the hard drive.
3. Run the following command:

   ```
   OEMLogoD <RomFileName> <NewOEMImageFileName> [/F or /FN or /N]
   ```

4.7.4.2 Changing the OEM Logo for Microsoft Windows* 2000 / 2003 / XP

1. Boot to Microsoft Windows 2000/2003/XP.
2. Download OEMLOGO.exe, Rombuild.exe, RomFile, and NewOEMlogoImage to the hard drive.
3. Run the following command:

   ```
   OEMLogo <RomFileName> <NewOEMImageFileName> [/F or /FN or /N]
   ```

4.8 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 buffer according to [PMM]. 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, checking each 2 KB boundary from C0000h to EFFFFh. The system vendor can place a signature within the user binary to distinguish it from other option ROMs.

Intel provides the tools and reference code to help OEMs build a user binary. The user binary must adhere to the following requirements:

- In order to be recognized by the BIOS and protected from runtime memory managers, the user binary must have an option ROM header (55AA, size).
- The system BIOS performs a scan of the user binary area at predefined points during POST. Mask bits must be set within the user binary to inform the BIOS if an entry point exists for a given time during POST.
- The system state must be preserved by the user binary.
- User binary code must be relocatable. It will be located within the first Megabyte. The user binary code should not make any assumptions about the value of the code segment.
- User binary code will always be executed from RAM and never from flash.
- The code in user binary should not hook critical interrupts, should not re-program the chipset and should not take any action that affects the correct functioning of the system BIOS.

The BIOS copies the user binary into system memory before the first scan point. If the user binary reports that it does not contain runtime code, it is located in conventional memory (0 - 640 KB).

Reporting that the user binary is POSTed has only the advantage that it does not use up limited option ROM space, and more option ROM space can be used for other devices. If user binary code is required at run-time, it is copied to the option ROM space. At each scan-point during POST, the system BIOS determines if the scan-point has a corresponding user binary entry point to transfer control to.

To determine this, the bitmap at byte 4 of the header is tested against the current mask bit that has been determined / defined by the scan point. If the bitmap has the appropriate bit set, the mask is placed in AL and execution is passed to the address computed by (ADR(Byte 5)+5*scan sequence #).

During execution, the user binary may access 11 bytes of Extended BIOS Data Area RAM (EBDA). The segment of the EBDA can be found at address 40:0e. Offset 18 to offset 21h is available for the user binary. The BIOS also reserves eight CMOS bits for the user binary. These bits are in a region of CMOS that does not have a checksum, with default values of zero, and will always be located in the first bank of CMOS. These bits are contiguous, but are not in a

fixed location. Upon entry into the user binary, DX contains a ‘token’ that points to the reserved bits.

4.9 Operating System Boot, Sleep, and Wake

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 1 MB). 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” in the INT 15h, function E820h.

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.

There are three runtime components to ACPI:

- **ACPI Tables**: These tables describe the interfaces to the hardware. ACPI tables can make use of a p-code type of language, the interpretation of which is performed by the operating system. The operating system contains and uses an ACPI Machine Language (AML) interpreter that executes procedures encoded in AML and stored in the ACPI tables. AML is a compact, tokenized, abstract machine language. The tables contain information about power management capabilities of the system, APICs, and bus structure. The tables also describe control methods that operating systems can use to change PCI interrupt routing, control legacy devices in Super I/O, find out the cause of wake events, and handle PCI hot plugging, if applicable.
- **ACPI Registers**: The constrained part of the hardware interface, described (at least in location) by the ACPI tables.

- **ACPI BIOS**: This is the code that boots the machine and implements interfaces for sleep, wake, and some restart operations. The ACPI Description Tables are also provided by the ACPI BIOS.

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.

4.9.3 Sleep and Wake Functionality

The BIOS supports a front 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 platform supports a front 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 front panel NMI button. The NMI button may not be provided on all front 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.

4.9.4 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.

4.9.5 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.

4.9.6 On to Off (OS present)

If an operating system is loaded, the power button switch 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.

4.9.7 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.

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

Table 46. 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 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.

4.10.1 Operating Model

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

Table 47. 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.	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.

4.10.2 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)	

4.10.3 Password Clear Jumper

If the user or administrator password(s) is lost or forgotten, moving the password clear jumper (J17) 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.

4.11 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

4.11.1 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).

5. Platform Management

The server boards support the Intel onboard platform instrumentation level of management. Integrated onto the server board is a National Semiconductor* PC87431 Mini-BMC (mBMC) that supports the functionality of the Essentials level of management. These server boards do not support the Flexible Management Connector that supports the optional Professional or Advanced Intel® Management Modules.

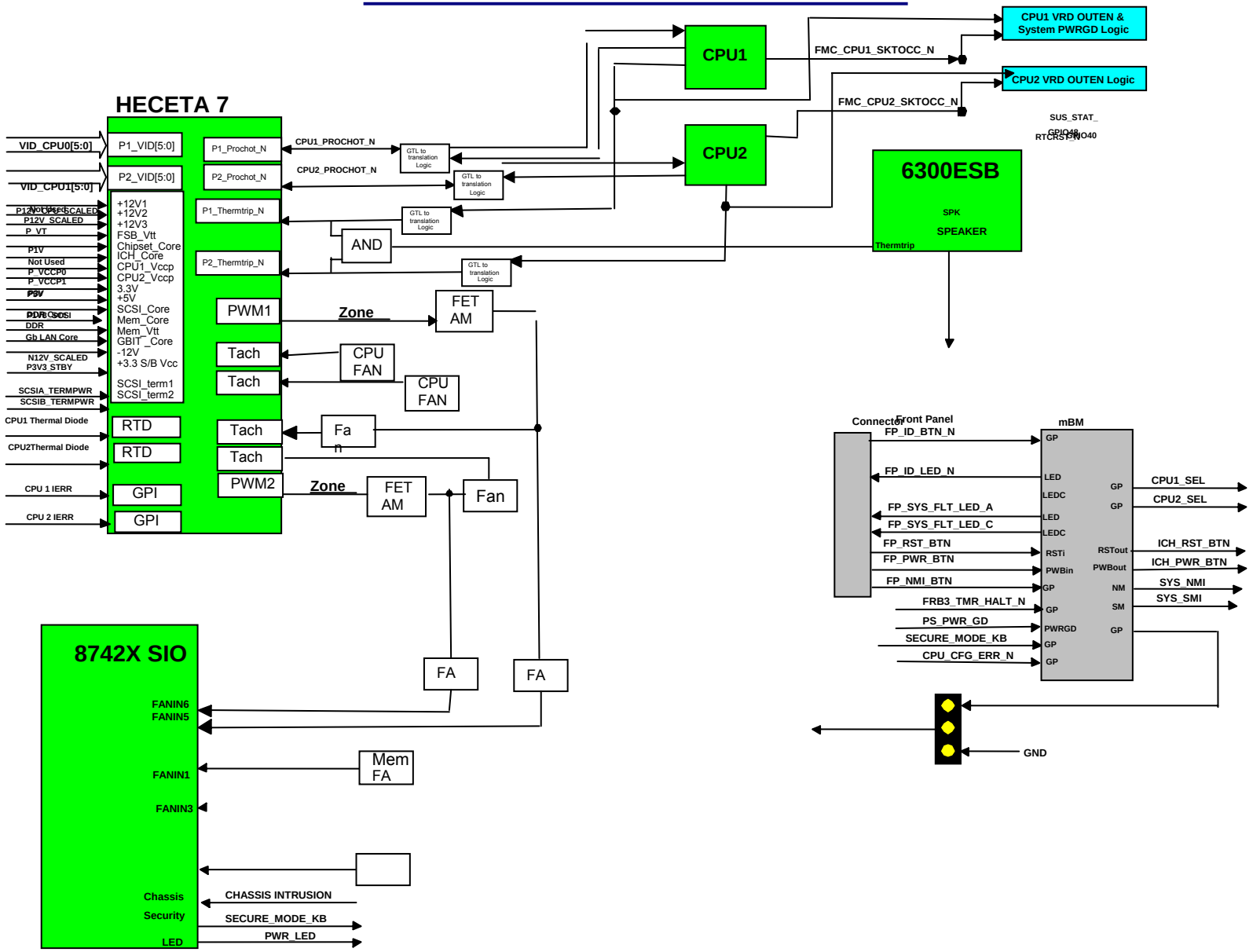


Figure 13. Block Diagram of Platform Managment Architecture

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 (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 server board RTC alarm signal, and power on request messages from the auxiliary IPMB connector and PCI SMBus.
- Onboard NICs which support IPMI-over-LAN and LAN Alerting, Wake-On LAN, and Magic Packet operation.
- Emergency management port
- IPMB
- PCI SMBus, is certain logic and private busses used for power control
- IPMB isolation circuit
- System Status/Fault LED on the front panel
- System Identify LED

5.1.2 IPMI Messaging, Commands, and Abstractions

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.*

Most of the 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 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 are 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 mBMC 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 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.

5.1.4 Private Management Buses

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 server board 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.

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

5.1.5 Mini-Baseboard Management Controller

At the heart of platform management is a management controller. To support the onboard platform instrumentation management model, the server boards incorporate the National Semiconductor* PC87431 Mini-BMC (mBMC).

The mBMC 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 operating system.

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 and 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). Standard and Advanced 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 are the common features supported by the mBMC.

- Power system
- System reset control
- System initialization
- Watchdog timer
- System event log
- Sensor data record (SDR) repository
- Field replaceable unit (FRU) inventory device
- NMI generation
- SMI generation
- Self test
- Secure mode
- Boot options

5.2 Onboard Platform Instrumentation Features and Functionality

The National Semiconductor* PC87431 management controller is an Application Specific Integrated Circuit (ASIC) with many peripheral devices embedded into it. The mBMC contains the logic needed for controlling the system, monitoring the sensors, and communicating with other systems and devices via various external interfaces.

The following figure is a 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.

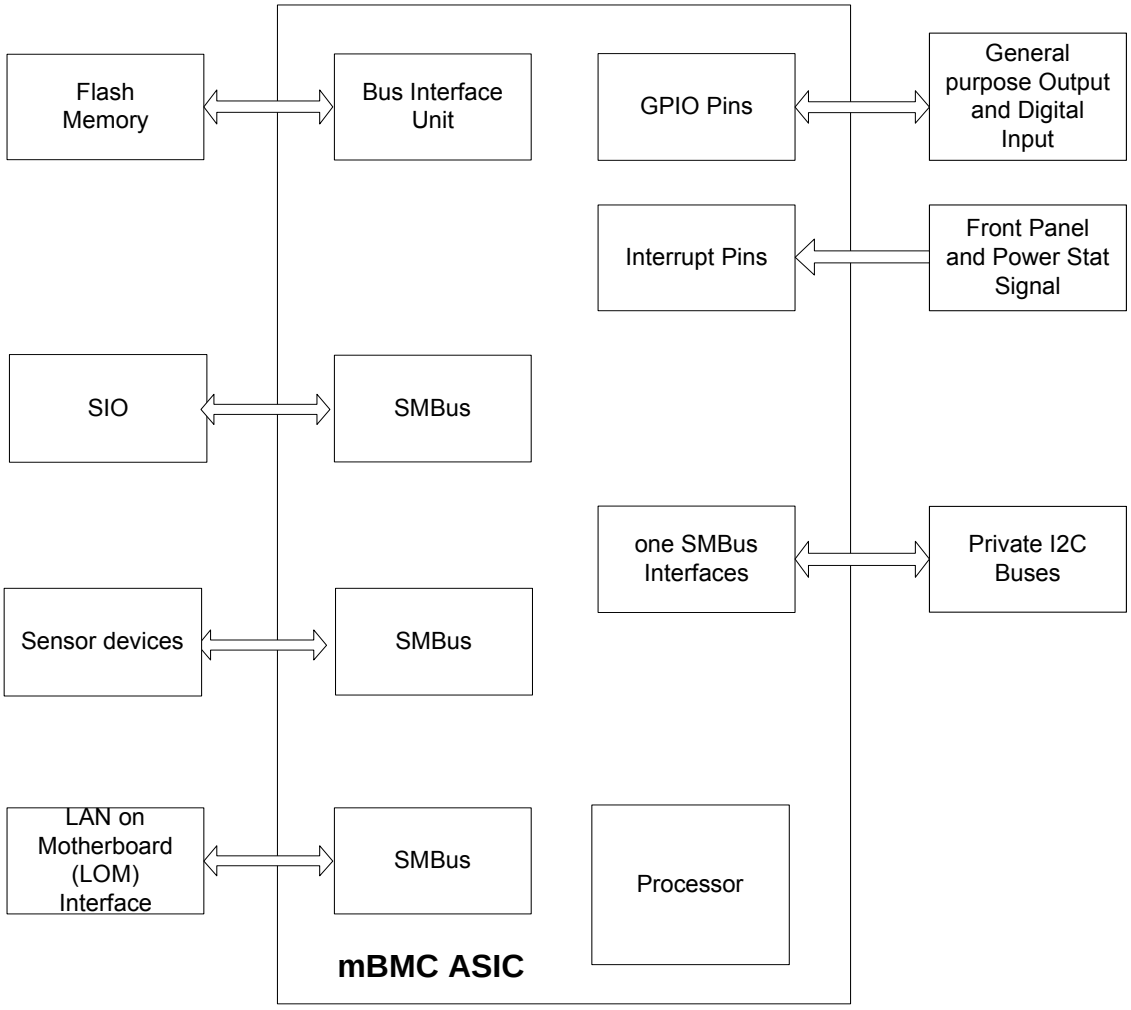


Figure 14. mBMC in a Server Management System

5.2.1 mBMC Self-test

The mBMC performs various tests as part of its initialization. If a failure is determined, the mBMC stores the error internally. A failure may be caused by a corrupt mBMC FRU, SDR, or SEL. The IPMI 1.5 *Get Self Test Results* command can be used to return the first error detected.

Executing the *Get Self Test Results* command causes the mBMC self-test to be run. It is strongly recommended to reset the mBMC via a server power cycle afterwards.

5.2.2 SMBus Interfaces

The mBMC incorporates one slave and two master-only SMBus interfaces. The mBMC interfaces with the host through the slave SMBus interface. It interfaces with the LAN On Motherboard (LOM) and peripherals through the two independent master bus interfaces.

5.2.3 External Interface to mBMC

Figure 15 shows the data/control flow to and within the functional modules of the mBMC. External interfaces from the host system, LOM, and peripherals, interact with the mBMC through the corresponding interface modules as shown.

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. GPIO pins are available and are used for various input and output functions. Dedicated LED lines are used for LED/color control.

Built into the mBMC are the control functions for both the power supply and front panel.

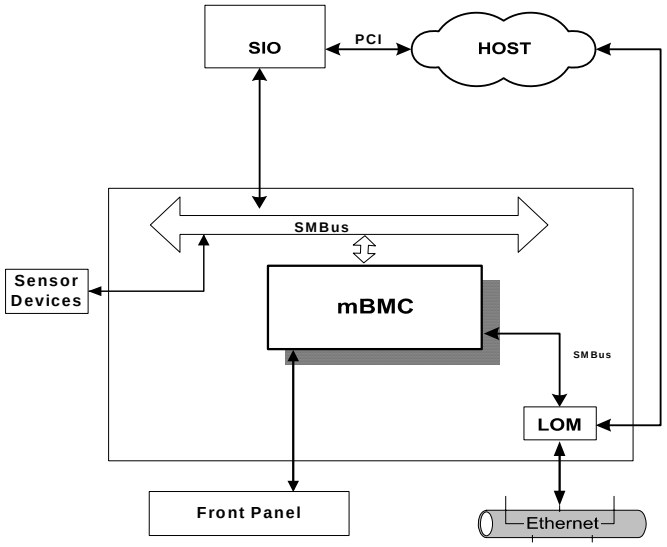


Figure 15. External Interfaces to mBMC

5.2.3.1 Private Management I²C Buses

The mBMC implements a single private management bus. The mBMC is the sole master on this bus. External agents must use the mBMC *Master Write/Read I²C* command if they require direct communication with a device on this bus. In addition, the mBMC provides a *Reserve Device* command that gives an external agent exclusive access to a specific device for a selectable time.

5.2.4 Messaging Interfaces

This section describes the supported mBMC communication interfaces:

- Host SMS interface via SMBus interface
- LAN interface using the LAN On Motherboard SMBus

5.2.4.1 Channel Management

The mBMC supports two channels:

- System interface
- 802.3 LAN

Table 48. Supported Channel Assigments

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

5.2.4.2 User Model

The mBMC supports one anonymous user (null user name) with a settable password. The IPMI command to set the password is supported.

5.2.4.3 Request/Response Protocol

All of the protocols used in the host interface and the LOM interface are Request/Response protocols. A Request Message is issued to an intelligent device, to which the device responds with a separate Response Message.

5.2.4.4 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.

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 if 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 down the bus periodically by extending the SMBus clock low interval (SCLH).
- 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 (“NAK”). This forces the host software to stop and restart the session.

For more information on read-write through SMBus, see the *System Management Bus* (SMBus) Specification 2.0.

5.2.4.5 LAN Interface

The server board supports one DPC LAN interface via a UDP port 26Fh. The mBMC supports a maximum of one simultaneous session across all authenticated channels. The server board implements gratuitous ARP support according to the IPMI 1.5 Specification.

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 readings
- 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 49. LAN Channel Capacity

LAN CHANNEL Capability	Options
Number of Sessions	1
Number of Users	1
User	Name NULL (anonymous)
User Password	Configurable
Privilege Levels	User, Operator, Administrator
Authentication Types	MD5
Number of LAN Alert Destinations	1
Address Resolution Protocol (ARP)	Gratuitous ARP

5.2.5 Direct Platform Control (IPMI over LAN)

Direct Platform Control provides a mechanism for delivering IPMI Messages directly to the management controllers via a LAN connection. The NICs and the management controllers remain active on standby power, enabling the IPMI Messaging when the system is powered up, powered down, and in a system sleep state. This allows a remote console application to be able to access the management controller capabilities, including:

- Power on/off and reset control with the ability to set BIOS boot flags
- FRU, SDR, and SEL access
- BMC configuration access
- Remote NMI generation
- Ability to transfer IPMI messages between the LAN interface and other interfaces, such as the System Interface, IPMB, and PCI SMBus. This capability enables messages to be delivered to system management software, and provides the ability to access sensors and FRU information on other management controllers.

IPMI Messages are encapsulated in a packet format called RMCP (Remote Management Control Protocol). The Distributed Management Task Force (DMTF) has defined RMCP for supporting pre-OS and OS-absent management. RMCP is a simple request-response protocol that can be delivered using UDP datagrams. IPMI-over-LAN uses version 1 of the RMCP protocol and packet format.

UDP port 26Fh is a ‘well known port’ address that is specified to carry RMCP (Remote Management Control Protocol) formatted UDP datagrams. The onboard Intel network interface controllers contain circuitry that enables detecting and capturing RMCP packets that are received on Port 26Fh and making them available to the management controller via a ‘side-band’ interface that is separate from the PCI interface to the NIC. Similarly, the management controller can use the side-band interface to send packets from Port 26Fh, as shown in the following figure.

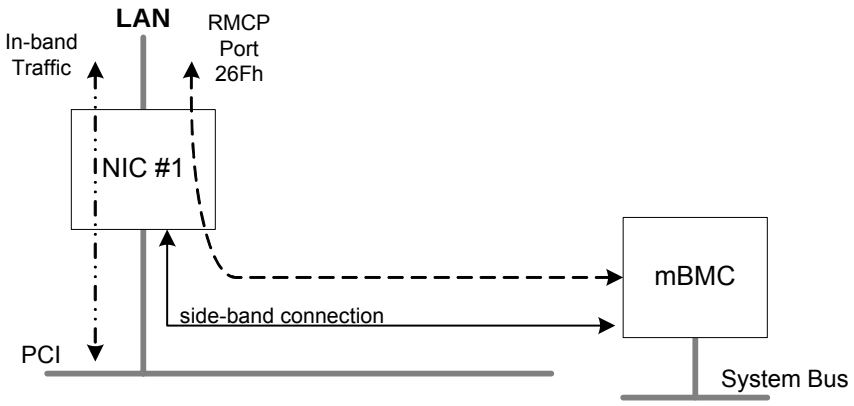


Figure 16. IPMI-over-LAN

RMCP includes a field that indicates the class of messages that can be embedded in an RMCP message packet. For RMCP version 1.0, the defined classes are IPMI, ASF, and OEM. IPMI-over-LAN uses the IPMI class to transfer IPMI Messages encapsulated in RMCP packets. Intelligent Platform Management Interface v1.5 Specification specifies the packet formats and commands used to perform IPMI Messaging on LAN via RMCP.

The management controller transmits to other port addresses as needed. For example, LAN Alerts, which are sent as SNMP Traps, can be transmitted to the SNMP Trap 'well known' port address, 162 (0A2h).

5.2.5.1 LAN Channel Specifications

The following table presents the minimum support that will be provided. Note that system management software and utilities may not use all the available management controller options and capabilities. For detailed technical information on the operation of the LAN channel operation and LAN Alerting, refer to Intelligent Platform Management Interface v1.5 specification.

Table 50. LAN Channel Specifications

Configuration Capability	Options	Description/Notes
Channel Access Modes	always-active, disabled	This option determines when the BMC can be accessed via IPMI Messaging over LAN.
Number of Sessions	1	The number of simultaneous sessions that can be supported is shared across the LAN and serial/modem channels.
Number of Users	1	User information is a resource that is shared across the LAN and serial/modem channels.
Configurable User Names	No	User information is a resource that is shared across the LAN and serial/modem channels.
Configurable User Passwords	Yes	
Privilege Levels	User, Operator, Administrator	

Configuration Capability	Options	Description/Notes
IPMI Message Authentication Type Support	MD5	
Number of LAN Alert destinations	1	
PET Acknowledge support	Yes	
Gratuitous ARP Support	Yes	

5.2.5.2 LAN Drivers and Setup

The IPMI-over-LAN feature must be used with the appropriate Intel NIC Driver, and the NIC correctly configured in order for DPC LAN operation to occur transparently to the operating system and network applications. If an incorrect driver or NIC configuration is used, it is possible to get driver timeouts when the IPMI-over-LAN feature is enabled.

5.2.5.3 BIOS Boot Flags

A remote console application can use the IPMI *Set System Boot Options* command to configure a set of BIOS boot flags and boot initiator parameters that are held by the management controller. These parameters include information that identifies the party that initiated the boot, plus flags and other information that can be used to direct the way booting proceeds after a system reset or power-up. For example, the system can be configured to boot normally, boot using PXE, boot to a diagnostic partition, etc.

5.2.5.4 Boot Flags and LAN Console Redirection

The system BIOS includes a LAN Console Redirection capability. This capability can only be directed to one IP Address at a time. Thus, the boot flags and boot initiator information are also used to tell the BIOS where to send LAN Console Redirection.

5.2.6 Wake On LAN / Power On LAN and Magic Packet Support

The server board supports Wake On LAN / Power On LAN capability using the onboard network interface chips or an add-in network interface card. An add-in network card can deliver the wake signal to the server board via the PME signal on the PCI bus. The actual support for Magic Packet and/or packet filtering for Wake On LAN / Power On LAN is provided by the NIC. The server board handles the corresponding wake signal.

5.2.6.1 Wake On LAN in S4/S5

A configuration option is provided that allows the onboard NICs to be enabled to wake the system in an S4/S5 state, even if the operating system disabled Wake-On-LAN when it powered down the system. This provides an option for users who want to use standard, but non-secure, WOL capability for operations such as after-hours maintenance. Note that the DPC LAN capability provides a secure system power-up, plus the ability to provide BIOS boot options, by sending authenticated IPMI messages directly to the BMC via the onboard NICs.

WOL from S5 is enabled/Disabled via BIOS option. When the function is enabled, the relevant register in SMRAM will have the corresponding value saved at every late POST, which will determine whether the system can be woken up on LAN from S5 after power off.

5.2.7 Watchdog Timer

The mBMC implements an IPMI 1.5-compatible watchdog timer. See the IPMI specification for details. SMI and NMI pre-timeout actions are supported, as are hard reset, power down, and power cycle timeout actions.

5.2.8 System Event Log (SEL)

The mBMC implements the logical system event log device as specified in the *Intelligent Platform Management Interface Specification, Version 1.5.* The SEL is accessible via all communication transports. In this way, the SEL information can be accessed while the system is down by means of out-of-band interfaces. The maximum SEL size that is supported by mBMC is 92 entries.

Supported commands are:

- Get SEL Info
- Reserve SEL
- Get SEL Entry
- Add SEL Entry
- Clear SEL
- Get SEL Time
- Set SEL Time

5.2.8.1 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. It is read using the *Get SEL Time* command and set using the *Set SEL Time* command. 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.*

After a mBMC reset or power up, 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 time via the *Set SEL Time* command. The mBMC maintains this time, incrementing it once per second, until the mBMC is reset or the time is changed via another *Set SEL Time* command.

If the RTC changes during system operation, system management software must synchronize the mBMC time with the system time. If this is not done, the system should be reset so that BIOS will pass the new time to the mBMC.

5.2.9 Sensor Data Record (SDR) Repository

The mBMC includes built-in sensor data records that provide platform management capabilities (sensor types, locations, event generation and access information). The SDR repository is accessible via all communication transports. This way, out-of-band interfaces can access the SDR repository information if the system is down.

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. It supports low-going and high-going sensor devices.

5.2.9.1 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 initializes, or when the system boots, the initialization agent scans the SDR repository and configures the sensors referenced by the SDRs. This includes setting sensor thresholds, enabling/disabling sensor event message scanning, and enabling/disabling sensor event messages.

5.2.10 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.

5.2.11 Event Filtering and Alerting

The mBMC implements the following IPMI 1.5 alerting features:

- PEF
- Alert over LAN

5.2.11.1 Platform Event Filtering (PEF)

The mBMC monitors platform health and logs failure events into the SEL. The platform event filtering 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 shut-down
- Power cycle
- Reset
- Diagnostic Interrupt
- Alert

The mBMC maintains an Event Filter table with 30 entries that is used to select the actions to perform. Also maintained is a 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 as shipped entry configuration should not be modified or those behaviors will be changed.*

Each time the PEF module receives either an externally or internally generated event message, 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. If a combination of actions is identified, such as power down, power cycle, and/or reset actions, the action are performed according to PEF Action Priorities. Action priorities are outlined in the table below.

Note: *An action that has changed from delayed to non-delayed, or an action whose delay time has been reduced has a higher priority. Each generated event is logged by SEL.*

Table 51. PEF Action Priorities

Action	Priority	Delayed	Type	Note
Power-down	1	Yes	PEF Action	
Soft shut-down	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.
NMI	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.
IPMB message event	8	No	OEM PEF Action	When selected, always occurs immediately after detection of a critical event.

Table 52. mBMC Factory Default Event Filters

Event Filter #	Offset Mask	Events
1	Non-critical	Voltage Assert
2	Non-critical	Voltage Deassert
3	Critical	Voltage Assert
4	Critical	Voltage Deassert
5	Critical	PS Soft Fail Assert
6	Critical	PS Soft Fail Deassert
7	Critical	Proc 1-2 Thermal Trip Assert
8	Critical	Proc 1-2 Thermal Trip, Config Error & IERR Deassert
9	Degraded	Proc 1-2 FRB3 Assert

Event Filter #	Offset Mask	Events
10	Degraded	Proc 1-2 FRB3 Deassert
11	Degraded	Proc 1-2 Hot Assert
12	Degraded	Proc 1-2 Hot Deassert
13	Critical	FP NMI Assert
14	Critical	FP NMI Deassert
15	Non Critical	SCSI Terminator Fail Assert
16	Non Critical	SCSI Terminator Fail Deassert
17	N/A	ID Button Assert
18	N/A	ID Button Deassert
19	Critical	Fan Speed Assert
20	Critical	Fan Speed Deassert
21	Non Critical	Fan Speed Assert
22	Non Critical	Fan Speed Deassert
23	Critical	Temperature Assert
24	Critical	Temperature Deassert
25	Non Critical	Temperature Assert
26	Non Critical	Temperature Deassert
27	Critical	Proc 1-2 IERR Assert
28	Critical	CPU Configuration Error
29	N/A	Reserved for ISM
30	N/A	Reserved for ISM

5.2.11.2 Alert over LAN

LAN alerts are sent as SNMP traps in ASF formatted Platform Event Traps to a specified alert destination. The Alert over LAN feature is used to send either Platform Event Trap 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 the LAN channel specified for the platform. LAN alerts can be used by PEF to send out alerts to selected destination when ever an event matches an event filter table entry For more information on LAN alerts, see the *IPMI Specification v1.5*.

5.2.11.3 System Identification in Alerts

The PET alert format used in PPP and LAN Alerting contains a system GUID field that can be used to uniquely identify the system that raised the alert. In addition, since the PET is carried in a UDP packet, the alerting system's IP Address is also present.

5.2.11.4 Platform Alerting Setup

The management controller provides commands via the System Interface that support setting/retrieving the alerting configuration LAN alerting in mBMC NV storage.

The user does not typically deal with filter contents directly. Instead, the Server Setup Utility provides a user interface that allows the user to select among a fixed set of pre-configured event filters.

The following list presents the type of alerting configuration options that are provided:

- Enabling / disabling PEF.
- Configuring Alert actions.
- Selecting which pre-configured events trigger an alert.
- Configuring the alert destination information, including LAN addresses.

5.2.11.5 Alerting On Power Down Events

A watchdog power-down event alert is sent after the power down so that the alert does not delay the power-down action.

5.2.11.6 Alerting On System Reset Events

The alerting process must complete before the system reset is completed. This is done to simplify timing interactions between the mBMC and BIOS initialization after a system reset.

5.2.11.7 Alert-in-Progress Termination

An alert in progress will be terminated by a system reset or power on, or by disabling alerting via commands to the management controller.

5.2.12 NMI Generation

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 front panel Diagnostic Interrupt (NMI) button has been pressed.
- A PEF table entry matching an event where the filter entry has the NMI action indicated.
- A processor IERR or Thermal Trip (if the mBMC is so configured).
- Watchdog timer pre-timeout expiration with NMI pre-timeout action enabled.

The mBMC-generated NMI pulse duration is 200ms. This time is chosen to try to avoid the BIOS missing the NMI if the BIOS is in the SMI Handler and the SMI Handler is masking the NMI.

Once an NMI has been generated by the mBMC, the mBMC will not generate another until the system has been reset or powered down except that enabling NMI via an *NMI Enable/Disable* command will re-arm the NMI.

The mBMC captures the NMI source(s) and makes that information available via a *Get NMI Source* command. Reading the NMI source information causes it to be cleared. A second *Set NMI Source* command can be used by other agents, such as the BIOS SMI Handler, to register NMI sources when they detect NMI generating errors. Operating system NMI handlers that save

the system crash state can use the *Get NMI Source* command to determine and save the cause of the NMI.

5.2.13 SMI Generation

The mBMC can generate an SMI due to watchdog timer pre-timeout expiration with SMI pre-timeout interrupt specified. The SMI generation is software configurable. The above conditions may or may not be enabled to cause an SMI.

5.3 Platform Management Interconnects

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 and is used to request power state changes (asserted = request *Power On*). The *Power Good* signal from the chassis power subsystem indicates current the power state (asserted = power is on).

Figure 17 shows the power supply control signals and their sources. To turn the system on, the mBMC asserts the *Power On* signal and waits for the *Power Good* signal to assert in response, indicating that DC power is on.

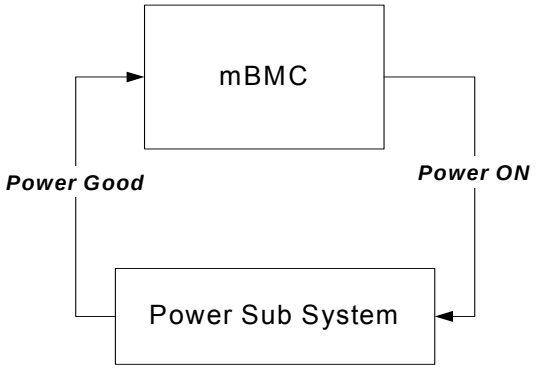


Figure 17. Power Supply Control Signals

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 that the mBMC uses to detect either power subsystem failure or loss of AC power. If AC power is suddenly lost, the mBMC:

- Immediately asserts system reset
- Powers down the system
- Waits for configured system off time (depending on configuration)
- Attempts to power the system on (depending on configuration)

5.3.1.1 Power-up Sequence

When turning on the system power in response to one of the event occurrences listed in Table 53 below, the mBMC executes the following procedure:

- The mBMC asserts *Power On* and waits for the power subsystem to assert *Power Good*. The system is held in reset.
- The mBMC sends a *Set ACPI Power State* command, indicating an S0 state to all management controllers whose SDR management device records indicate that they should receive the notification.
- The mBMC initializes all sensors to their *Power On* initialization state. The Init Agent is run.
- The mBMC attempts to boot the system by running the FRB algorithm.

5.3.1.2 Power-down Sequence

To power down the system, the mBMC effectively performs the sequence of power-up steps in reverse order. This operation can be initiated by one of the event occurrences listed in Table 53 and proceeds as follows:

- The mBMC asserts system reset (de-asserts *Power Good*).
- If enabled, the mBMC sends a *Set ACPI Power State* command, indicating an S0 state to all management controllers whose SDR management device records indicate that they should receive the notification.
- The mBMC de-asserts the *Power On* signal.
- The power subsystem turns off system power upon de-assertion of the *Power On* signal.

5.3.1.3 Power Control Sources

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

Table 53. Power Control Initiators

#	Source	External Signal Name or Internal Subsystem	Capabilities
1	Power Button	FP Power button	Turns power on or off
2	mBMC Watchdog Timer	Internal mBMC timer	Turns power off, or power cycle
3	Platform Event Filtering	PEF	Turns power off, or power cycle
4	Command	Routed through command processor	Turns power on or off, or power cycle
5	Power state retention	Implemented via mBMC internal logic	Turns power on when AC power returns
6	Chipset	Sleep S5	Turns power on or off

5.3.2 System Reset Control

5.3.2.1 Reset Signal Output

The mBMC asserts the *System Reset* signal on the server board 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.

To reset the system without a power state change, the mBMC:

- Asserts the *System Reset* signal.
- Holds this state for as long as the reset button is pushed. When a command is used to generate a system reset, the state is held for the stipulated time.
- De-asserts the *System Reset* signal.

5.3.2.2 Reset Control Sources

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

Table 54. System Reset Sources and Actions

#	Reset Source	System Reset?	mBMC Reset
1	Standby power comes up	No (no DC power)	Yes
2	Main system power comes up	Yes	No
3	Reset button or in-target probe (ITP) reset	Yes	No
4	Warm boot (example: DOS Ctrl-Alt-Del)	Yes	No
5	Command to reset the system	Yes	No
6	Set Processor State command	Yes	No
7	Watchdog timer configured for reset	Yes	No
8	FRB3 failure	Yes	No
9	PEF action	Optional	No

5.3.3 Temperature-based Fan Speed Control

Server board hardware implements an ambient-temperature-based Fan Speed control that is part of *normal system operation.* With one exception, the management controller does not participate in fan speed control. The feature allows the server board to drive different fan speeds based on various temperature measurements in order to lower the acoustic noise of the system.

The ambient-temperature thresholds at which the fan speed increases does not correspond to a non-critical (warning) condition for the fan because the fan's state is still 'OK' from the system point-of-view.

The server board has two analog fan speed signals that are driven by pulse-width modulator (PWM) circuits by the server board hardware. These signals can be driven to several levels according to temperature measurements. Multiple bytes of a Sensor Initialization Table are used to hold parameters that set the temperature thresholds and corresponding PWM duty cycles. This SDR or table is loaded as part of the server board configuration.

The management controller firmware expects to find an LM30 temperature sensor on the front panel board. Thus, the ambient temperature-based fan speed control capability is not enabled by default for SE7320SP2 or SE7525GP2 as a server board-only product, but can be enabled via a management controller configuration change.

5.3.3.1 Fan Kick-start

Some fans may not begin rotating unless started at high speed. To ensure that the fans start, the server board hardware will start and run the fans at high speed for a brief interval following system power up.

5.3.4 Front Panel Control

The mBMC provides the main 'front panel control' functions. These include control of the system Power Button, Reset Button, Diagnostic Interrupt (Front Panel NMI) Button, System Identify Button, System ID LED, Status/Fault LED, and Chassis Intrusion Switch. Front panel control also includes the front panel lockout features.

5.3.4.1 Power Button

After de-bouncing the front panel *Power Button* signal, the mBMC routes the signal state directly to the chipset *Power Button* signal input. If the chipset has been initialized by the BIOS, the chipset responds to the assertion of the signal by requesting a power state change. It reacts to the press of the switch, not the release of it.

The *Power Button* signal toggles the system power. The *Power Button* signal to the mBMC is activated by a momentary contact switch on the front 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. The chipset responds to the assertion of the signal. It responds to the press of the switch, not the release of it.

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

In the case of simultaneous button presses, the *Power Button* action takes priority over all other buttons. For example, if the sleep button is depressed for one second and then the *Power Button* is pressed and released, the system powers down. 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.

5.3.4.2 Reset Button

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

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

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

5.3.4.3 Diagnostic Interrupt Button (Front 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 the NMI, which can be used as an OEM-specific diagnostic front panel interface.

The Diagnostic Interrupt button is connected to the mBMC through the front panel connector. A Diagnostic Interrupt button press causes the mBMC to generate a system NMI pulse whose duration is platform-specific and unrelated to the button press duration.

This generates an event (NMI button sensor) and PEF OEM action causes NMI generation.

5.3.4.4 Chassis ID Button and LED

The front panel interface supports a *Chassis Identify* Button and a corresponding Blue *Chassis Identify* LED. A second Blue Chassis Identify LED is mounted on the back edge of the server board where it may be visible when viewed from the back of an integrated system.

The LED can provide a mechanism for identifying one system out of a group of identical systems in a high density rack environment

The Chassis Identify LED can be turned on either locally via the push-button signal, or by local or remote software using the IPMI *Chassis Identify* command. The following list summarizes the Chassis Identify Push-button and LED operation:

- The Identify signal state is preserved on Standby power across system power-on/off and system hard resets. It is not preserved if A/C power is removed. The initial LED state is Off when A/C power is applied.
- The IPMI *Chassis Identify* command can also be used to control the LED. If a the *Chassis Identify* command is used to turn the LED On, the command will automatically time out and turn off the LED unless another *Chassis Identify* command to turn on the LED is received. The default timeout for the command is 15 seconds. The server board supports the optional command parameter to allow the timeout to be set anywhere from 1 to 255 seconds.
- The optional timeout parameter in the *Chassis Identify* command also allows software to tell the LED to go off immediately.

- The Chassis Identify Push-button works using a “push-on/push-off” operation. Each press of the push-button toggles the LED signal state between on and off. If the pushbutton is used to turn the LED on, it will stay on indefinitely, until either the button is pressed again or a *Chassis Identify* or *Chassis Identify LED* command causes the LED to turn off.

Table 55. Chassis ID LEDs

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

5.3.4.5 Status/Fault LED

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

Table 56. Fault/Status LED

Color	Condition	When
Green	Solid	System Ready
	Blink	System Ready, but degraded. CPU fault, DIMM killed
Amber	Solid	Critical Failure: critical fan, voltage, temperature state
	Blink	Non-Critical Failure: non-critical fan, voltage, temperature state
Off	Solid	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.
- Power subsystem failure. The BMC asserts this failure whenever it detects a power control fault (e.g., the BMC detects that the system power is remaining on even though the BMC has deasserted the signal to turn off power to the system). A hot-swap backplane would use the *Set Fault Indication* command to indicate when one or more of the drive fault status LEDs are asserted on the hot-swap backplane.
- The system is unable to power up due to incorrectly installed processor(s), or processor incompatibility.
- Satellite controller sends a critical or non-recoverable state, via the *Set Fault Indication* command to the BMC.
- “Critical Event Logging” errors, including: System Memory Uncorrectable ECC error and Fatal/Uncorrectable Bus errors, such as PCI SERR and PERR.

on-Critical Condition

- Temperature, voltage, or fan non-critical threshold crossing
- Chassis intrusion
- Satellite controller sends a non-critical state, via the *Set Fault Indication* command, to the mBMC
- *Set Fault Indication* command from system BIOS. The BIOS may use the *Set Fault Indication* command to indicate additional, non-critical status such as system memory or CPU configuration changes.

Degraded Condition

- One or more processors are disabled by Fault Resilient Boot (FRB) or BIOS
- BIOS has disabled or mapped out some of the system memory

5.3.4.6 Chassis Intrusion Switch

Some platforms support chassis intrusion detection. On these platforms, the mBMC monitors the state of the *Chassis Intrusion* signal and makes the status of the signal available via the *Get Chassis Status* command and *Physical Security* sensor state. If enabled, a chassis intrusion state change causes the mBMC to generate a *Physical Security* sensor event message with a *General Chassis Intrusion* offset.

5.3.4.7 Front Panel Lockout

The management controller monitors a ‘Secure Mode’ signal from the keyboard controller on the server board. When the Secure Mode signal is asserted, the management controller may lock out the ability to power down or reset the system using the power or reset push buttons, respectively. Secure Mode may also block the ability to initiate a sleep request using the sleep push-button.

The management controller generates a ‘Secure Mode Violation Attempt’ event message if an attempt it made to power-down, sleep, or reset the system using the push buttons while Secure Mode is active.

The mBMC will prevent the system from powering up via button press when either secure mode or the front panel lockout I/O signal is asserted.

5.3.5 Secure Mode Operation

Secure mode is a signal from the SIO/keyboard controller. Power and reset buttons are locked out, except for the NMI and Chassis ID buttons. A security violation event is generated if buttons are pressed while secure mode active.

The Secure Mode feature allows the front panel switches and other system resources to be protected against unauthorized use or access. Secure Mode is enabled and controlled via the *Set Secure Mode Options* command.

If it is enabled, Secure Mode can be controlled via the *Secure Mode KB* signal from the keyboard controller. When Secure Mode is active, pressing a protected front panel switch generates a Secure Mode Violation event. Specifically, this generates an assertion of the *Secure Mode Violation Attempt* offset of the mBMC's *Platform Security Violation Attempt* sensor.

The Secure Mode state is cleared whenever AC power or system power is applied, when a system reset occurs, or when a mBMC reset occurs. The Secure Mode state includes the bits that specify the actions that are to be taken when Secure Mode is active, as well as the *Force Secure Mode On* bit.

The *Set Secure Mode Options* command allows specific front panel switches to be protected irrespective of Secure Mode state. See the command definition in the IPMI v1.5 specification for details.

The NMI switch can be locked using the *Set Secure Mode Options* command but is never protected by Secure Mode. This allows a system to be recovered from a hung state when Secure Mode is active

5.3.6 FRU Information

The platform management architecture supports providing FRU (field replaceable unit) information for the server board and major replaceable modules in the chassis. 'Major Module' is defined as any circuit board in the system containing active electronic circuitry.

FRU information includes board serial number, part number, name, asset tag, and other information. FRUs that contain a management controller use the controller to provide access to the FRU information. FRUs that lack a management controller can make their FRU information available via a SEEPROM directly connected to the IPMB or a private I^2C bus. This allows the system integrator to provide a chassis FRU device without having to implement a management controller. This information can be accessed via IPMI FRU commands or using Master Write-Read commands.

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 via all interfaces.

5.3.6.1 mBMC FRU Inventory Area Format

The mBMC FRU inventory area format follows the Platform Management FRU Information Storage Definition. Refer to *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 are written. This includes the common header area. Applications cannot relocate or resize any FRU inventory areas.

The server board's FRU information is kept in the mBMC internal flash memory.

5.4 Sensors

5.4.1 Sensor Type Codes

The following tables list the sensor identification numbers and information regarding the sensor type, name, supported thresholds, assertion and deassertion information, and a brief description of the sensor purpose. Refer to the *Intelligent Platform Management Interface Specification, Version 1.5*, for sensor and event/reading-type table information.

- **Sensor Type**
  The Sensor Type references the values enumerated in the *Sensor Type Codes* table in the IPMI specification. It provides the context in which to interpret the sensor, e.g., the physical entity or characteristic that is represented by this sensor.
- **Event/Reading Type**
  The Event/Reading Type references values from the *Event/Reading Type Code Ranges* and *Generic Event/Reading Type Codes* tables in the *IPMI specification*. Note that digital sensors are a specific type of discrete sensors, which have only two states.
- **Event Offset/Triggers**
  Event Thresholds are supported event generating thresholds for threshold types of sensors.
  - [u,l][nr,c,nc] upper nonrecoverable, upper critical, upper noncritical, lower nonrecoverable, lower critical, lower noncritical
  - uc, lc upper critical, lower critical

  Event Triggers are supported event generating offsets for discrete type sensors. The offsets can be found in the *Generic Event/Reading Type Codes* or *Sensor Type Codes* tables in the IPMI specification, depending on whether the sensor event/reading type is generic or a sensor specific response.
- **Assertion/Deassertion Enables**
  Assertions and Deassertion indicators reveals the type of events the sensor can generate:
  - As: Assertions
  - De: Deassertion
- Readable Value / Offsets
  - Readable Value indicates the type of value returned for threshold and other non-discrete type sensors.
  - Readable Offsets indicates the offsets for discrete sensors that are readable via the *Get Sensor Reading* command. Unless otherwise indicated, all Event Triggers are readable, i.e., *Readable Offsets* consists of the reading type offsets that do not generate events.
- **Event Data**
  This is the data that is included in an event message generated by the associated sensor. For threshold-based sensors, the following abbreviations are used:
  - R: Reading value
  - T: Threshold value

The following table lists the core sensors located within the mBMC. These sensors are fixed and hard-coded. They cannot be modified by a user.

Table 57. mBMC Built-in Sensors

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 Specific 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

The following table shows the server board/platform sensors that are supported by the mBMC.

Table 58. Built-in Platform Sensors

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	Event Data
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 Specific 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

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	Event Data
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 Hard Reset Warm Reset	As	–	Trig Offset
System PEF Event	07h	System Event 12h	Sensor Specific 6Fh	PEF Action	As	–	Trig Offset
Platform Alert	08h	Platform Alert 24h	Sensor Specific 6Fh	Platform Event Trap generated	As	–	Trig Offset

Table 59. External Platform Sensors

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	09h	Physical Security 05h	Sensor Specific 6Fh	General Chassis Intrusion	As	General Chassis Intrusion	Trig Offset	X	02
CPU1 12v	0Ah	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
CPU2 12v	0Bh	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
BB +1.5V	0Ch	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
BB +1.8V	0Dh	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
BB +3.3V	0Eh	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
BB +5V	0Fh	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
BB +12V	10h	Voltage 02h	Threshold 01h	[u,l][nr, 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
BB -12V	11h	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
FSB Vtt	12h	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
MCH Vtt	13h	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
SCSI Core(1.8v)	14h	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
Proc1 VCCP	15h	Voltage 02h	Generic 03h	State Asserted	As & De	Discrete	R, T	Fault LED Action	02
Proc2 VCCP	16h	Voltage 02h	Generic 03h	State Asserted	As & De	Discrete	R, T	Fault LED Action	02
Tach Fan 1 (Front 1)	17h	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
Tach Fan 2 (Front 2)	18h	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
Tach Fan 3 (Front 3)	19h	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
Tach Fan 4 (Front 4)	1Ah	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
Tach Fan 5 (Rear 1)	1Bh	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
Tach Fan 6 (Rear 2)	1Ch	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
Proc1 IERR	1Dh	Processor 07h	Sensor Specific 6Fh	IERR	As	–	Trig Offset	–	02
Proc2 IERR	1Eh	Processor 07h	Sensor Specific 6Fh	IERR	As	–	Trig Offset	–	02
Proc1 Thermal trip	1Fh	Processor 07h	Sensor Specific 6Fh	Thermal Trip	As	–	Trig Offset	Fault LED Action	02
Proc2 Thermal trip	20h	Processor 07h	Sensor Specific 6Fh	Thermal Trip	As	–	Trig Offset	Fault LED Action	02
Proc1 Throttle	21h	Temp 01h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	Trig Offset	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
Proc2 Throttle	22h	Temp 01h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	Trig Offset	Fault LED Action	01
Diagnostic Interrupt Button	23h	Critical Interrupt 13h	Sensor Specific 6Fh	FP NMI Button	As	–	Trig Offset	NMI Pulse	02
Chassis Identify Button	24h	Button 14h	Generic 03h	Sate Deasserted State Assert	As	–	Trig Offset	ID LED Action	02
Proc1 Fan	25h	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
Proc2 Fan	26h	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
Proc1 Core temp	27h	Temp 01h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
Proc2 Core temp	28h	Temp 01h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action	01
CPU Configuration Error	29h	Processor 07h	Generic 03h	State Asserted	As & De	Discrete	R, T	Fault LED Action	02
System Temp	2A	Temp 01h	Threshold 01h	State Asserted	As & De	Discrete	R, T	Fault LED Action	02

6. Error Reporting and Handling

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 are either displayed to the video screen, or if an error has occurred prior to video initialization, errors are reported through a series of audio beep codes.

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

6.1 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.

6.1.1 Error Sources and Types

One of the major requirements of server management is to correctly and consistently handle system errors. System errors 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.

6.1.2 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.

6.1.2.1 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#.

6.1.2.2 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.

6.1.2.3 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.

6.1.2.4 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 mBMC. The BIOS does not generate an SMI to the host processor for these types of system events.

6.1.2.5 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 mBMC to log the watchdog timer reset event.

If an operating system 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 mBMC for a watchdog reset event as the system reboots, and then log this event in the SEL.

6.1.2.6 Boot Event

The BIOS downloads the system date and time to the mBMC 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.

6.1.2.7 Logging Format Conventions

The BIOS event log data in the SEL complies with the IPMI specification. IPMI requires use of all but two bytes in each event log entry, called Event Data 2 and Event Data 3. An event generator can specify that these bytes contain OEM-specified values. The system BIOS uses these two bytes to record additional information about the error.

The format of the OEM data bytes (Event Data 2 and Event Data 3) for memory errors, PCI bus errors and FRB2 errors is described here. This format is supported by all platforms that are IPMI version 1.0 (or later) compliant.

Bits 3:1 of the generator ID field define the format revision. The system software ID is a 7-bit quantity. For events covered in this document, the system software IDs will be within the range 0x18-0x1F. System software ID of 0x18 indicates that OEM data byte 2 and 3 are encoded using data format scheme revision 0. Note that the system software IDs in the range 0x10-0x1f are reserved for the SMI handler. The IPMI specification reserves two distinct ranges for the BIOS and the SMI handler. Since the distinction between the two is not very important, we use the same values of generator ID's for the BIOS as well as the SMI handler. Technically, the FRB-2 event is not logged by the SMI handler, but it will use the same generator ID range as memory errors.

6.1.3 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.

6.2 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.

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

Most POST error codes are logged in the system event log.

6.2.1 POST Error Codes and Messages

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 system cannot boot unless the error is corrected.

Table 60. POST Error Messages and Handling

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

Error Code	Error Message	Response
0010	Floppy Controller Failure	Pause
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

Error Code	Error Message	Response
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
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 and Secondary BIOS ID's do not match.	Pause
8601	Override jumper is set to force boot from lower bank of flash ROM.	Pause
8602	Watchdog timer expired (secondary BIOS may be bad!).	Pause
8603	Secondary BIOS checksum fail.	Pause

6.2.2 Boot Block Error Beep Codes

Table 61. 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

6.2.3 POST Error Beep Codes

The following table lists the POST error beep codes. Before system video initialization, the BIOS uses these beep codes to inform users of error conditions.

Table 62. POST Error Beep Codes

Number of Beeps	Description
1	Memory refresh timer error
2	Parity error in base memory (first 64 KB block)
3	Base memory read / write test error
4	Server board 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

6.2.3.1 Troubleshooting BIOS Beep Codes

Table 63. 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 server board beyond all hope, eliminate the possibility of interference by a malfunctioning add-in card. Remove all expansion cards except the video adapter. - If beep codes are generated even when all other expansion cards are absent, consult your system manufacturer's technical support. - If 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.

6.2.4 "POST Error Pause" Option

In case of POST error(s) that occur during system boot-up, the BIOS will stop and wait for the user to press an appropriate key before booting the operating system or entering BIOS setup.

The user can override this option by setting "POST Error Pause" to "disabled" in the BIOS setup Advanced menu page. If the "POST Error Pause" option is set to "disabled", the system will boot the operating system without user intervention. The default value setting for this option is "enabled".

6.3 Checkpoints

6.3.1 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 65 provides a list of the Port 80 codes and the corresponding task description.

6.3.2 Diagnostic LEDs

All port 80 codes are displayed using the diagnostic LEDs found on the back edge of the server board. 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 64. 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	

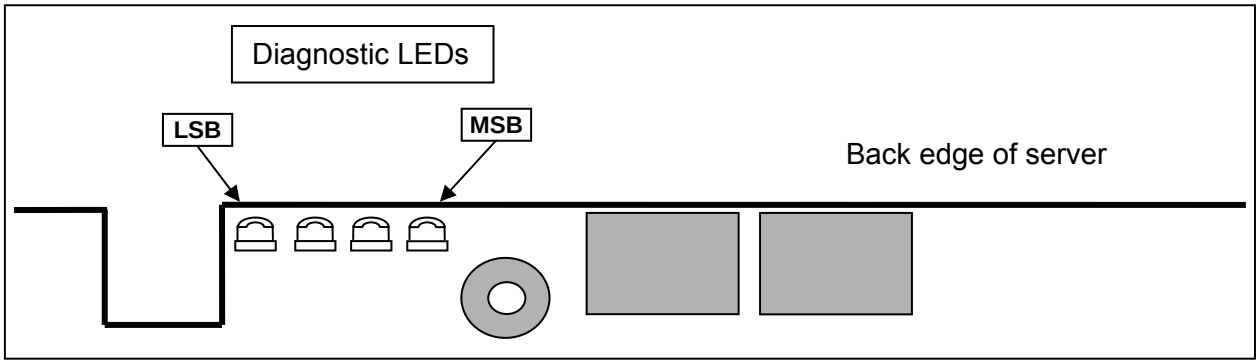


Figure 18. Location of Diagnostic LEDs (Example only)

6.3.3 POST Code Checkpoints

Table 65. POST Code Checkpoints

Checkpoint	Diagnostic LED Decoder G=Green, R=Red, A=Amber MSB			LSB	Description
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
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.

Checkpoint	Diagnostic LED Decoder G=Green, R=Red, A=Amber				Description
	MSB			LSB	
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.
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.

Checkpoint	Diagnostic LED Decoder G=Green, R=Red, A=Amber				Description
	MSB			LSB	
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).

6.3.4 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 66. 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 4 GB 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.
D4	R	A	OFF	R	Test base 512 KB memory. Adjust policies and cache first 8 MB. 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.

Checkpoint	Diagnostic LED Decoder G=Green, R=Red, A=Amber				Description
	MSB			LSB	
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 1 MB 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.

6.3.5 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 67. 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.
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.

6.3.6 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 68. 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.

6.3.7 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 69. 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.

6.3.8 Memory Error Codes

Table 70. 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
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)

6.4 Intel® Light-Guided Diagnostics

The server board provides system fault/status LEDs in many areas of the board to alert users to a particular failure or status of a component on the board. There are fault LEDs for the memory DIMMs and processors, and status LEDs for 5-volt stand-by and system state.

7. Connector Definitions and Pin-outs

7.1 Main Power Connector

The main power supply connection is obtained using the 24-pin connector. The following table defines the pin-outs of the connector.

Table 71. Power Connector Pin-out (J12)

Pin	Signal	18 AWG Color	Pin	Signal	18 AWG Color
1*	+3.3VDC	Orange	13	+3.3VDC	Orange
	3.3V RS	Orange (24AWG)	14	-12VDC	Blue
2	+3.3VDC	Orange	15	COM	Black
3*	COM	Black	16	PSON#	Green
	COM RS	Black (24AWG)	17	COM	Black
4*	+5VDC	Red	18	COM	Black
	5V RS	Red (24AWG)	19	COM	Black
5	COM	Black	20	Reserved	N.C.
6	+5VDC	Red	21	+5VDC	Red
7	COM	Black	22	+5VDC	Red
8	PWR OK	Gray	23	+5VDC	Red
9	5 VSB	Purple	24	COM	Black
10	+12V3	Yellow			
11	+12V3	Yellow			
12	+3.3VDC	Orange			

Table 72. Auxiliary Signal Connector (J5)

Pin	Signal	24 AWG Color
1	I2C Clock	White
2	I2C Data	Yellow
3	Reserved	N.C.
4	COM	Black
5	3.3RS	Orange

Table 73. Auxiliary CPU Power Connector Pin-out (J22)

Pin	Signal	18 AWG color	Pin	Signal	18 AWG Color
1	COM	Black	5*	+12V1	White
2	COM	Black		12V1 RS	Yellow (24AWG)
3	COM	Black	6	+12V1	White
4	COM	Black	7	+12V2	Brown
			8*	+12V2	Brown
				12V2 RS	Yellow (24AWG)

7.2 Memory Module Connector

The board has four DDR266/333 DIMM connectors and supports registered ECC DDR modules (Rev 1.0).

Table 74. DIMM Connectors (J16,J18,J20,J21)

Pin	Front	Pin	Front	Pin	Front	Pin	Back	Pin	Back	Pin	Back
1	VREF	32	A5	62	VDDQ	93	VSS	124	VSS	154	/RAS
2	DQ0	33	DQ24	63	/WE	94	DQ4	125	A6	155	DQ45
3	VSS	34	VSS	64	DQ41	95	DQ5	126	DQ28	156	VDDQ
4	DQ1	35	DQ25	65	/CAS	96	VDDQ	127	DQ29	157	/CS0
5	DQS0	36	DQS3	66	VSS	97	DM0	128	VDDQ	158	*/CS1
6	DQ2	37	A4	67	DQS5	98	DQ6	129	DM3	159	DM5
7	VDD	38	VDD	68	DQ42	99	DQ7	130	A3	160	VSS
8	DQ3	39	DQ26	69	DQ43	100	VSS	131	DQ30	161	DQ46
9	NC	40	DQ27	70	VDD	101	NC	132	VSS	162	DQ47
10	/RESET	41	A2	71	*/CS2	102	NC	133	DQ31	163	*/CS3
11	VSS	42	VSS	72	DQ48	103	*A13	134	CB4	164	VDDQ
12	DQ8	43	A1	73	DQ49	104	VDDQ	135	CB5	165	DQ52
13	DQ9	44	CB0	74	VSS	105	DQ12	136	VDDQ	166	DQ53
14	DQS1	45	CB1	75	*/CK2	106	DQ13	137	CK0	167	NC
15	VDDQ	46	VDD	76	*CK2	107	DM1	138	/CK0	168	VDD
16	*CK1	47	DQS8	77	VDDQ	108	VDD	139	VSS	169	DM6
17	*/CK1	48	A0	78	DQS6	109	DQ14	140	DM8	170	DQ54
18	VSS	49	CB2	79	DQ50	110	DQ15	141	A10	171	DQ55
19	DQ10	50	VSS	80	DQ51	111	*CKE1	142	CB6	172	VDDQ
20	DQ11	51	CB3	81	VSS	112	VDDQ	143	VDDQ	173	NC
21	CKE0	52	BA1	82	VDDID	113	*BA2	144	CB7	174	DQ60
22	VDDQ	KEY		83	DQ56	114	DQ20	KEY		175	DQ61
23	DQ16	53	DQ32	84	DQ57	115	A12	145	VSS	176	VSS
24	DQ17	54	VDDQ	85	VDD	116	VSS	146	DQ36	177	DM7

Pin	Front	Pin	Front	Pin	Front	Pin	Back	Pin	Back	Pin	Back
25	DQS2	55	DQ33	86	DQS7	117	DQ21	147	DQ37	178	DQ62
26	VSS	56	DQS4	87	DQ58	118	A11	148	VDD	179	DQ63
27	A9	57	DQ34	88	DQ59	119	DM2	149	DM4	180	VDDQ
28	DQ18	58	VSS	89	VSS	120	VDD	150	DQ38	181	SA0
29	A7	59	BA0	90	NC	121	DQ22	151	DQ39	182	SA1
30	VDDQ	60	DQ35	91	SDA	122	A8	152	VSS	183	SA2
31	DQ19	61	DQ40	92	SCL	123	DQ23	153	DQ44	184	VDDSPD

Note:

* These pins are not used in this module.

7.3 Processor Socket

The board has two Socket 604 processor sockets. The following table provides the processor socket pin numbers and pin names:

Table 75. Socket 604 Processor Socket Pin-out (J36, J37)

Pin No	Pin Name	Pin No	Pin Name	Pin No	Pin Name	Pin No	Pin Name	Pin No	Pin Name
A1	VID5	D29	VCC	K3	VCC	T29	VSS	AB3 [2]	BSEL1
A2	VCC	D30	VSS	K4	VSS	T30	VCC	AB4	VCCA
A3	SKTOCC#	D31	VCC	K5	VCC	T31	VSS	AB5	VSS
A4	VTT	E1	VTTEN	K6	VSS	U1	VCC	AB6	D63#
A5	VSS	E2	VCC	K7	VCC	U2	VSS	AB7	PWRGOOD
A6	A32#	E3	VID1	K8	VSS	U3	VCC	AB8	VCC
A7	A33#	E4	BPM5#	K9	VCC	U4	VSS	AB9	DBI3#
A8	VCC	E5	IERR#	K23	VCC	U5	VCC	AB10	D55#
A9	A26#	E6	VCC	K24	VSS	U6	VSS	AB11	VSS
A10	A20#	E7	BPM2#	K25	VCC	U7	VCC	AB12	D51#
A11	VSS	E8	BPM4#	K26	VSS	U8	VSS	AB13	D52#
A12	A14#	E9	VSS	K27	VCC	U9	VCC	AB14	VCC
A13	A10#	E10	AP0#	K28	VSS	U23	VCC	AB15	D37#
A14	VCC	E11	BR2# [1]	K29	VCC	U24	VSS	AB16	D32#
A15	FORCEPR#	E12	VTT	K30	VSS	U25	VCC	AB17	D31#
A16	IEST_BUS	E13	A28#	K31	VCC	U26	VSS	AB18	VCC
A17	LOCK#	E14	A24#	L1	VSS	U27	VCC	AB19	D14#
A18	VCC	E15	VSS	L2	VCC	U28	VSS	AB20	D12#
A19	A7#	E16	COMP1	L3	VSS	U29	VCC	AB21	VSS
A20	A4#	E17	VSS	L4	VCC	U30	VSS	AB22	D13#
A21	VSS	E18	DRDY#	L5	VSS	U31	VCC	AB23	D9#
A22	A3#	E19	TRDY#	L6	VCC	V1	VSS	AB24	VCC
A23	HITM#	E20	VCC	L7	VSS	V2	VCC	AB25	D8#
A24	VCC	E21	RS0#	L8	VCC	V3	VSS	AB26	D7#

Pin No	Pin Name	Pin No	Pin Name	Pin No	Pin Name	Pin No	Pin Name	Pin No	Pin Name
A25	TMS	E22	HIT#	L9	VSS	V4	VCC	AB27	VSS
A26	Reserved	E23	VSS	L23	VSS	V5	VSS	AB28	NC
A27	VSS	E24	TCK	L24	VCC	V6	VCC	AB29	NC
A28	VCC	E25	TDO	L25	VSS	V7	VSS	AB30	VCC
A29	VSS	E26	VCC	L26	VCC	V8	VCC	AB31	VSS
A30	VCC	E27	FERR#/PBE#	L27	VSS	V9	VSS	AC1	Reserved
A31	VSS	E28	VCC	L28	VCC	V23	VSS	AC2	VSS
B1	VIDPWRGD	E29	VSS	L29	VSS	V24	VCC	AC3	VCC
B2	VSS	E30	VCC	L30	VCC	V25	VSS	AC4	VCC
B3	VID4	E31	VSS	L31	VSS	V26	VCC	AC5	D60#
B4	VTT	F1	VCC	M1	VCC	V27	VSS	AC6	D59#
B5	OTDEN	F2	VSS	M2	VSS	V28	VCC	AC7	VSS
B6	VCC	F3	VID0	M3	VCC	V29	VSS	AC8	D56#
B7	A31#	F4	VCC	M4	VSS	V30	VCC	AC9	D47#
B8	A27#	F5	BPM3#	M5	VCC	V31	VSS	AC10	VCC
B9	VSS	F6	BPM0#	M6	VSS	W1	VCC	AC11	D43#
B10	A21#	F7	VSS	M7	VCC	W2	VSS	AC12	D41#
B11	A22#	F8	BPM1#	M8	VSS	W3	Reserved	AC13	VSS
B12	VTT	F9	GTLREF	M9	VCC	W4	VSS	AC14	D50#
B13	A13#	F10	VTT	M23	VCC	W5	BCLK1	AC15	DP2#
B14	A12#	F11	BINIT#	M24	VSS	W6	TESTHI0	AC16	VCC
B15	VSS	F12	BR1#	M25	VCC	W7	TESTHI1	AC17	D34#
B16	A11#	F13	VSS	M26	VSS	W8	TESTHI2	AC18	DP0#
B17	VSS	F14	ADSTB1#	M27	VCC	W9	GTLREF	AC19	VSS
B18	A5#	F15	A19#	M28	VSS	W23	GTLREF	AC20	D25#
B19	REQ0#	F16	VCC	M29	VCC	W24	VSS	AC21	D26#
B20	VCC	F17	ADSTB0#	M30	VSS	W25	VCC	AC22	VCC
B21	REQ1#	F18	DBSY#	M31	VCC	W26	VSS	AC23	D23#
B22	REQ4#	F19	VSS	N1	VCC	W27	VCC	AC24	D20#
B23	VSS	F20	BNR#	N2	VSS	W28	VSS	AC25	VSS
B24	LINT0	F21	RS2#	N3	VCC	W29	VCC	AC26	D17#
B25	PROCHOT#	F22	VCC	N4	VSS	W30	VSS	AC27	DBI0#
B26	VCC	F23	GTLREF	N5	VCC	W31	VCC	AC28	NC
B27	VCCSENSE	F24	TRST#	N6	VSS	Y1	VSS	AC29	NC
B28	VSS	F25	VSS	N7	VCC	Y2	VCC	AC30	SLEW_CTRL
B29	VCC	F26	THERMTRIP#	N8	VSS	Y3	Reserved	AC31	VCC
B30	VSS	F27	A20M#	N9	VCC	Y4	BCLK0	AD1	VCCPLL
B31	VCC	F28	VSS	N23	VCC	Y5	VSS	AD2	VCC
C1	OPTIMIZED/ COMPAT#	F29	VCC	N24	VSS	Y6	TESTHI3	AD3	VSS
C2	VCC	F30	VSS	N25	VCC	Y7	VSS	AD4	VCCIOPLL
C3	VID3	F31	VCC	N26	VSS	Y8	RESET#	AD5	TESTHI5

Pin No	Pin Name	Pin No	Pin Name	Pin No	Pin Name	Pin No	Pin Name	Pin No	Pin Name
C4	VCC	G1	VSS	N27	VCC	Y9	D62#	AD6	VCC
C5	VTT	G2	VCC	N28	VSS	Y10	VTT	AD7	D57#
C6	RSP#	G3	VSS	N29	VCC	Y11	DSTBP3#	AD8	D46#
C7	VSS	G4	VCC	N30	VSS	Y12	DSTBN3#	AD9	VSS
C8	A35#	G5	VSS	N31	VCC	Y13	VSS	AD10	D45#
C9	A34#	G6	VCC	P1	VSS	Y14	DSTBP2#	AD11	D40#
C10	VTT	G7	BOOT_SELECT	P2	VCC	Y15	DSTBN2#	AD12	VTT
C11	A30#	G8	VCC	P3	VSS	Y16	VCC	AD13	D38#
C12	A23#	G9	VSS	P4	VCC	Y17	DSTBP1#	AD14	D39#
C13	VSS	G23	LINT1	P5	VSS	Y18	DSTBN1#	AD15	VSS
C14	A16#	G24	VCC	P6	VCC	Y19	VSS	AD16	COMP0
C15	A15#	G25	VSS	P7	VSS	Y20	DSTBP0#	AD17	VSS
C16	VCC	G26	VCC	P8	VCC	Y21	DSTBN0#	AD18	D36#
C17	A8#	G27	VSS	P9	VSS	Y22	VCC	AD19	D30#
C18	A6#	G28	VCC	P23	VSS	Y23	D5#	AD20	VCC
C19	VSS	G29	VSS	P24	VCC	Y24	D2#	AD21	D29#
C20	REQ3#	G30	VCC	P25	VSS	Y25	VSS	AD22	DBI1#
C21	REQ2#	G31	VSS	P26	VCC	Y26	D0#	AD23	VSS
C22	VCC	H1	VCC	P27	VSS	Y27	THERMDA	AD24	D21#
C23	DEFER#	H2	VSS	P28	VCC	Y28	THERMDC	AD25	D18#
C24	TDI	H3	VCC	P29	VSS	Y29	NC	AD26	VCC
C25	VSS	H4	VSS	P30	VCC	Y30	VCC	AD27	D4#
C26	IGNNE#	H5	VCC	P31	VSS	Y31	VSS	AD28	NC
C27	SMI#	H6	VSS	R1	VCC	AA1	VCC	AD29	NC
C28	VCC	H7	VCC	R2	VSS	AA2	VSS	AD30	VCC
C29	VSS	H8	VSS	R3	VCC	AA3	BSEL0 [2]	AD31	VSS
C30	VCC	H9	VCC	R4	VSS	AA4	VCC	AE2	VSS
C31	VSS	H23	VCC	R5	VCC	AA5	VSSA	AE3	VCC
D1	VCC	H24	VSS	R6	VSS	AA6	VCC	AE4	SMB_PRT
D2	VSS	H25	VCC	R7	VCC	AA7	TESTHI4	AE5	TESTHI6
D3	VID2	H26	VSS	R8	VSS	AA8	D61#	AE6	SLP#
D4	STPCLK#	H27	VCC	R9	VCC	AA9	VSS	AE7	D58#
D5	VSS	H28	VSS	R23	VCC	AA10	D54#	AE8	VCC
D6	INIT#	H29	VCC	R24	VSS	AA11	D53#	AE9	D44#
D7	MCERR#	H30	VSS	R25	VCC	AA12	VTT	AE10	D42#
D8	VCC	H31	VCC	R26	VSS	AA13	D48#	AE11	VSS
D9	AP1#	J1	VSS	R27	VCC	AA14	D49#	AE12	DBI2#
D10	BR3# [1]	J2	VCC	R28	VSS	AA15	VSS	AE13	D35#
D11	VSS	J3	VSS	R29	VCC	AA16	D33#	AE14	VCC
D12	A29#	J4	VCC	R30	VSS	AA17	VSS	AE15	Reserved
D13	A25#	J5	VSS	R31	VCC	AA1	D24#	AE16	Reserved

Pin No	Pin Name	Pin No	Pin Name	Pin No	Pin Name	Pin No	Pin Name	Pin No	Pin Name
D14	VCC	J6	VCC	T1	VSS	AA19	D15#	AE17	DP3#
D15	A18#	J7	VSS	T2	VCC	AA20	VCC	AE18	VCC
D16	A17#	J8	VCC	T3	VSS	AA21	D11#	AE19	DP1#
D17	A9#	J9	VSS	T4	VCC	AA22	D10#	AE20	D28#
D18	VCC	J23	VSS	T5	VSS	AA23	VSS	AE21	VSS
D19	ADS#	J24	VCC	T6	VCC	AA24	D6#	AE22	D27#
D20	BR0#	J25	VSS	T7	VSS	AA25	D3#	AE23	D22#
D21	VSS	J26	VCC	T8	VCC	AA26	VCC	AE24	VCC
D22	RS1#	J27	VSS	T9	VSS	AA27	D1#	AE25	D19#
D23	BPRI#	J28	VCC	T23	VSS	AA28	NC	AE26	D16#
D24	VCC	J29	VSS	T24	VCC	AA29	NC	AE27	VSS
D25	Reserved	J30	VCC	T25	VSS	AA30	VSS	AE28	Reserved
D26	VSSSENSE	J31	VSS	T26	VCC	AA31	VCC	AE29	Reserved
D27	VSS	K1	VCC	T27	VSS	AB1	VSS	AE30	NC
D28	VSS	K2	VSS	T28	VCC	AB2	VCC		

Notes:

1. These are “Reserved ” pins on the Intel® Xeon® processor. In systems utilizing the Intel Xeon processor, the system designer must terminate these signals to the processor VTT.

2. Server boards treating AA3 and AB3 as Reserved will operate correctly with a bus clock of 200 MHz.

3. The FC-mPGA2P package contains an extra pin (located at location AE30) compared to the INT-mPGA package. This additional pin serves as a keying mechanism to prevent the FC-mPGA2P package from being installed in the 603-pin socket. Since the additional contact for pin AE30 is electrically inert, the 604-pin socket will not have a solder ball at this location.

7.4 I²C Headers

Table 76. HSBP Header Pin-out (J54)

Pin	Signal Name	Description
1	HR_SMB_P5V_DAT	Data Line
2	GND	GROUND
3	HR_SMB_P5V_CLK	Clock Line
4	GND	GROUND

Table 77. HSBP Header Pin-out (J30)

Pin	Signal Name	Description
1	HR_SMB_P5V_DAT	Data Line
2	GND	GROUND
3	HR_SMB_P5V_CLK	Clock Line
4	GND	GROUND

Table 78. Remote Management Card Header Pin-out (J33)

Pin	Signal Name	Description
1	MBMC_SMB_PHL_DAT	Data Line
2	GND	GROUND
3	MBMC_SMB_PHL_CLK	Clock Line
4	P5V_STBY	POWER
5	NC	
6	NC	
7	NC	
8	NC	

7.5 PCI Slot Connector

There are three PCI buses implemented on the server board. PCI segment A supports 5V 32-bit/33 MHz PCI, segment B supports 3.3V 64-bit/66 MHz PCI-X, and segment C supports 3.3V PCI Express* operation. All segments support full-length PCI add-in cards. The pin-out for each segment is below.

Table 79. P32-A 5V 32-bit/33-MHz PCI Slot Pin-out (J10, J11)

Pin	Side B	Side A	Pin	Side B	Side A
1	-12V	TRST#	32	AD[17]	AD[16]
2	TCK	+12V	33	C/BE[2]#	+3.3V
3	Ground	TMS	34	Ground	FRAME#
4	TDO	TDI	35	IRDY#	Ground
5	+5V	+5V	36	+3.3V	TRDY#
6	+5V	INTA#	37	DEVSEL#	Ground
7	INTB#	INTC#	38	Ground	STOP#
8	INTD#	+5V	39	LOCK#	+3.3V
9	PRSNT1#	Reserved	40	PERR#	SMBCLK
10	Reserved	+5V (I/O)	41	+3.3V	SMBDAT
11	PRSNT2#	Reserved	42	SERR#	Ground
12	Ground	Ground	43	+3.3V	PAR
13	Ground	Ground	44	C/BE[1]#	AD[15]
14	Reserved	3.3Vaux	45	AD[14]	+3.3V
15	Ground	RST#	46	Ground	AD[13]
16	CLK	+5V (I/O)	47	AD[12]	AD[11]
17	Ground	GNT#	48	AD[10]	Ground
18	REQ#	Ground	49	Ground	AD[09]
19	+5V (I/O)	PME#	50	CONNECTOR KEY	
20	D[31]	AD[30]	51	CONNECTOR KEY	
21	AD[29]	+3.3V	52	AD[08]	C/BE[0]#
22	Ground	AD[28]	53	AD[07]	+3.3V

Pin	Side B	Side A	Pin	Side B	Side A
23	AD[27]	AD[26]	54	+3.3V	AD[06]
24	AD[25]	Ground	55	AD[05]	AD[04]
25	+3.3V	AD[24]	56	AD[03]	Ground
26	C/BE[3]#	IDSEL	57	Ground	AD[02]
27	AD[23]	+3.3V	58	AD[01]	AD[00]
28	Ground	AD[22]	59	+5V (I/O)	+5V (I/O)
29	AD[21]	AD[20]	60	ACK64#	REQ64#
30	AD[19]	Ground	61	+5V	+5V
31	+3.3V	AD[18]	62	+5V	+5V

Table 80. P64-B 3.3V 64-bit/66-MHz PCI-X Slot Pin-out (J8, J9)

Pin	Side B	Side A	Pin	Side B	Side A
1	-12V	TRST#	49	M66EN	AD[09]
2	TCK	+12V	50	Ground	Ground
3	Ground	TMS	51	Ground	Ground
4	TDO	TDI	52	AD[08]	C/BE[0]#
5	+5V	+5V	53	AD[07]	+3.3V
6	+5V	INTA#	54	+3.3V	AD[06]
7	INTB#	INTC#	55	AD[05]	AD[04]
8	INTD#	+5V	56	AD[03]	Ground
9	PRSNT1#	Reserved	57	Ground	AD[02]
10	Reserved	+3.3V (I/O)	58	AD[01]	AD[00]
11	PRSNT2#	Reserved	59	+3.3V (I/O)	+3.3V (I/O)
12	CONNECTOR KEY		60	ACK64#	REQ64#
13	CONNECTOR KEY		61	+5V	+5V
14	Reserved	3.3Vaux	62	+5V	+5V
15	Ground	RST#		CONNECTOR KEY	
16	CLK	+3.3V (I/O)		CONNECTOR KEY	
17	Ground	GNT#	63	Reserved	Ground
18	REQ#	Ground	64	Ground	C/BE[7]#
19	+3.3V (I/O)	PME#	65	C/BE[6]#	C/BE[5]#
20	AD[31]	AD[30] A	66	C/BE[4]#	+3.3V (I/O)
21	AD[29]	+3.3V	67	Ground	PAR64
22	Ground	AD[28]	68	AD[63]	AD[62]
23	AD[27]	AD[26]	69	AD[61]	Ground
24	AD[25]	Ground	70	+3.3V (I/O)	AD[60]
25	+3.3V	AD[24]	71	AD[59]	AD[58]
26	C/BE[3]#	IDSEL	72	AD[57]	Ground
27	AD[23]	+3.3V	73	Ground	AD[56]
28	Ground	AD[22]	74	AD[55]	AD[54]
29	AD[21]	AD[20]	75	AD[53]	+3.3V (I/O)

Pin	Side B	Side A	Pin	Side B	Side A
30	AD[19]	Ground	76	Ground	AD[52]
31	+3.3V	AD[18]	77	AD[51]	AD[50]
32	AD[17]	AD[16]	78	AD[49]	Ground
33	C/BE[2]#	+3.3V	79	+3.3V (I/O)	AD[48]
34	Ground	FRAME#	80	AD[47]	AD[46]
35	IRDY#	Ground	81	AD[45]	Ground
36	+3.3V	TRDY#	82	Ground	AD[44]
37	DEVSEL#	Ground	83	AD[43]	AD[42]
38	PCIXCAP	STOP#	84	AD[41]	+3.3V (I/O)
39	LOCK#	+3.3V	85	Ground	AD[40]
40	PERR#	SMBCLK	86	AD[39]	AD[38]
41	+3.3V	SMBDAT	87	AD[37]	Ground
42	SERR#	Ground	88	+3.3V (I/O)	AD[36]
43	+3.3V	PAR	89	AD[35]	AD[34]
44	C/BE[1]#	AD[15]	90	AD[33]	Ground
45	AD[14]	+3.3V	91	Ground	AD[32]
46	Ground	AD[13]	92	Reserved	Reserved
47	AD[12]	AD[11]	93	Reserved	Ground
48	AD[10]	Ground	94	Ground	Reserved

Table 81. PCI Express* Slot Pin-out (J13 for x4, J14 for x16)

Pin	Side B	Side A	Pin	Side B	Side A
1	+12V	PRSNT1#	42	HSION6	GND
2	+12V	+12V	43	GND	HSIP6
3	RSVD	+12V	44	GND	HSIN6
4	GND	GND	45	HSOP7	GND
5	SMCLK	TCK	46	HSON7	GND
6	SMDAT	TDI	47	GND	HSIP7
7	GND	TDO	48	PRSNT2#	HSIN7
8	+3.3V	TMS	49	GND	GND
			End of the x8 Connector		
9	TRST#	+3.3V	50	HSOP8	RSVD
10	+3.3AUX	+3.3V	51	HSON8	GND
11	WAKE#	PWRGD	52	GND	HSIP8
Mechanical Key					
12	RSVD	GND	53	GND	HSIN8
13	GND	REFCLK+	54	HSOP9	GND
14	HSOP0	REFCLK-	55	HSON9	GND
15	HSON0	GND	56	GND	HSIP9
16	GND	HSIP0	57	GND	HSIN9
17	PRSNT2#	HSIN0	58	HSOP10	GND

Pin	Side B	Side A	Pin	Side B	Side A
18	GND	GND	59	HSON10	GND
End of the x1 Connector					
19	HSOP1	RSVD	60	GND	HSIP10
20	HSON1	GND	61	GND	HSIN10
21	GND	HSIP1	62	HSOP11	GND
22	GND	HSIN1	63	HSON11	GND
23	HSOP2	GND	64	GND	HSIP11
24	HSON2	GND	65	GND	HSIN11
25	GND	HSIP2	66	HSOP12	GND
26	GND	HSIN2	67	HSON12	GND
27	HSOP3	GND	68	GND	HSIP12
28	HSON3	GND	69	GND	HSIN12
29	GND	HSIP3	70	HSOP13	GND
30	RSVD	HSIN3	71	HSON13	GND
31	PRSNT#2	GND	72	GND	HSIP13
32	GND	RSVD	73	GND	HSIN13
End of the x4 Connector					
33	HSOP4	RSVD	74	HSOP14	GND
34	HSON4	GND	75	HSON14	GND
35	GND	HSIP4	76	GND	HSIP14
36	GND	HSIN4	77	GND	HSIN14
37	HSOP5	GND	78	HSOP15	GND
38	HSON5	GND	79	HSON15	GND
39	GND	HSIP5	80	GND	HSIP15
40	GND	HSIN5	81	PRSNT2#	HSIN15
41	HSOP6	GND	82	RSVD	GND

7.6 Front Panel Connector

A standard SSI 34-pin header is provided to support a system front panel. The header contains reset, NMI, power control buttons, and LED indicators. The following table details the pin-out of this header.

Table 82. Front Panel 34-Pin Header Pin-out (J38)

Signal Name	Pin	Pin	Signal Name
ACPI_LEDgrn	1	2	SB5V
KEY	3	4	FAN_FAULT LED (NO SUPPORT) [1]
ACPI_LED amber	5	6	FAN_FAULT LED# (NO SUPPORT) [1]
HDD_LED	7	8	SYS_Status LED 2
HDD_LED#	9	10	SYS_Status LED#
PWR_BTN	11	12	NIC1 ACT_LED
PWR_BTN (GND)	13	14	NIC1 ACT_LED#
RESET switch	15	16	SMB SDA
RESET switch (GND)	17	18	SMB SCL
Sleep switch (NO SUPPORT) [1]	19	20	INDRUDER [1]
Sleep switch (GND) [1]	21	22	NIC2 ACT_LED
NMI switch#	23	24	NIC2 ACT_LED#
Key	25	26	Key
ID LED	27	28	P5V_STBY
ID LED#	29	30	SYS_Status LED 1
ID_BTN	31	32	NC
ID_BTN (GND)	33	34	NC

Note:

[1] => NC (no connect)

7.7 VGA Connector

The following table details the pin-out of the VGA connector. This connector is combined with COM1 connector.

Table 83. VGA Connector Pin-out (J4)

Signal Name	Pin	Pin	Signal Name
RED	B1	B9	Fused VCC (+5V) (NO SUPPORT)
GREEN	B2	B10	NC
BLUE	B3	B11	NC
NC	B4	B12	DDCDAT
GND	B5	B13	HSY
GND	B6	B14	VSY
GND	B7	B15	DDCCLK
GND	B8	B16	NC
		B17	NC

Note: NC (No Connect) t

7.8 NIC Connector

Table 84. NIC1 82541GI(10/100/1000) Connector Pin-out (JA1)

Signal Name	Pin	Pin	Signal Name
GND	1	9	MDI_3N
MDI_2N	2	10	MDI_0N
MDI_2P	3	11	MDI_0P
MDI_1P	4	12	GND
MDI_1N	5	13	ACT_L
GND	6	14	LINK_L
GND	7	15	LINK1000_L
MDI_3P	8	16	LINK100_L

7.9 IDE Connector

The board provides two 40-pin ATA-100 IDE connectors

Table 85. ATA 40-pin Connector Pin-out (J41, J43)

Pin	Signal Name	Pin	Signal Name
1	RESET#	2	GND
3	IDE_DD7	4	IDE_DD8
5	IDE_DD6	6	IDE_DD9
7	IDE_DD5	8	IDE_DD10
9	IDE_DD4	10	IDE_DD11
11	IDE_DD3	12	IDE_DD12
13	IDE_DD2	14	IDE_DD13
15	IDE_DD1	16	IDE_DD14
17	IDE_DD0	18	IDE_DD15
19	GND	20	KEY
21	IDE_DMAREQ	22	GND
23	IDE_IOW#	24	GND
25	IDE_IOR#	26	GND
27	IDE_IORDY	28	GND
29	IDE_DMAACK#	30	GND
31	IRQ_IDE	32	Test Point
33	IDE_A1	34	DIAG
35	IDE_A0	36	IDE_A2
37	IDE_DCS0#	38	IDE_DCS1#
39	IDE_HD_ACT#	40	GND

7.10 SATA Connectors

Table 86. SATA Connector Pin-out (J28, J32)

Pin	Signal Name
1	GND
2	S_TX_P
3	S_TX_N
4	GND
5	S_RX_N
6	S_RX_P
7	GND

7.11 USB Connector

The following table provides the pin-out for the dual external USB connectors.

Table 87. USB Connectors Pin-out (J3)

Pin	Signal Name
1	Fused VCC (+5V /w over current monitor of both port 3)
2	DATAN3 (Differential data line paired with DATAH3)
3	DATAP3 (Differential data line paired with DATAL3)
4	GND
5	Fused VCC (+5V /w over current monitor of both port 2)
6	DATAN2 (Differential data line paired with DATAH2)
7	DATAP2 (Differential data line paired with DATAL2)
8	GND
9	CTS_N
10	DSR_DCD
11	SIN
12	RI_N
13	GND
14	SIUT
15	DTR_N
16	RTS_N

A header on the server board provides an option to support one additional USB connector. The pin-out of the header is detailed in the following table.

Table 88. Optional USB Connection Header Pin-out (J31)

Signal Name	Pin	Pin	Signal Name
Fused VCC (+5V /w over current monitor of both port 1)	1	2	Fused VCC (+5V /w over current monitor of both port 0)
DATAN1	3	4	DATAN0
DATAP1	5	6	DATAP0
GND	7	8	GND
Key	9	10	NC

7.12 Floppy Connector

The board provides a standard 34-pin interface to the floppy drive controller. The following tables detail the pin-out of the 34-pin floppy connector.

Table 89. Legacy 34-pin Floppy Connector Pin-out (J47)

Signal Name	Pin	Pin	Signal Name
GND	1	2	FDDENSEL
GND	3	4	Unused
KEY	5	6	FDDRATE0
GND	7	8	FDINDEX#
GND	9	10	FDMTR0#
GND	11	12	FDR1#
GND	13	14	FDR0#
GND	15	16	FDMTR1#
Unused	17	18	FDDIR
GND	19	20	FDSTEP#
GND	21	22	FDWDATA#
GND	23	24	FDWGATE#
GND	25	26	FDTRK0#
Unused	27	28	FLWP#
GND	29	30	FRDATA#
GND	31	32	FHDSEL#
GND	33	34	FDSKCHG#

7.13 Serial Port Connector

Two serial ports are provided on the SE7320SP2 and Server Board SE7525GP2.

- A standard, external DB9 serial connector is located on the back edge of the server board to supply a Serial A interface. And this connector is combined with VGA connector (J4)
- A Serial B port is provided through a 9-pin header (J15) on the server board.

The following tables detail the pin-outs of these two ports.

Table 90. External DB9 Serial A Port Pin-out (J8A1)

Signal Name	Pin	Pin	Signal Name
SERIAL_DCD1_FB	T1	T6	SERIAL_DSR1_FB
SERIAL_RX1_FB	T2	T7	SERIAL_RTS1_FB
SERIAL_TX1_FB	T3	T8	SERIAL_CTS1_FB
SERIAL_DTR1_FB	T4	T9	SERIAL_RING1_FB
GND	T5		

Table 91. 9-pin Header Serial B Port Pin-out (J15)

Signal Name	Pin	Pin	Signal Name
SERIAL_DCD2_FB	1	2	SERIAL_DSR2_FB
SERIAL_RX2_FB	3	4	SERIAL_RTS2_FB
SERIAL_TX2_FB	5	6	SERIAL_CTS2_FB
SERIAL_DTR2_FB	7	8	SERIAL_RING2_FB
GND	9	10	Key

7.14 Keyboard and Mouse Connector

Two PS/2 ports are provided for use by a keyboard and a mouse. The following table details the pin-out of the PS/2 connectors.

Table 92. Keyboard and Mouse PS/2 Connectors Pin-out (J2)

PS/2 Connectors	Pin	Signal Name
Keyboard	1	KBDATA
	2	NC
	3	GND
	4	KMPWR
	5	KBCLK
	6	NC
Mouse	7	MSEDATA
	8	NC
	9	GND
	10	KMPWR
	11	MSECLK
	12	
	13,14,15,16,17	GND

7.15 Miscellaneous Headers

7.15.1 Fan Header

There are six 3-pin fan headers. All fan headers provide speed monitoring onboard. The fan headers are labeled, CPU_1 FAN and CPU_2 FAN, and SYS FAN_1 - 4. All fan headers have the same pin-out and are detailed below.

Table 93. Three-pin Fan Headers Pin-out (J51, J52, J7, J1, J45, J48)

Pin	Signal Name	Type	Description
1	Ground	Power	GROUND is the power supply ground
2	Fan Power	Power	Fan Power
3	Fan Tach	Out	FAN_TACH signal is connected to the Super I/O to monitor the FAN speed.

Table 94. Six-pin Fan headers Pin-out (J44, J46)

Pin	Signal Name	Type	Description
1	Ground	Power	GROUND is the power supply ground
2	Fan Power	Power	Fan Power
3	Fan Tach	Out	FAN_TACH signal is connected to the Super I/O to monitor the FAN speed.
4	Fan PWM	Out	Fan speed control
5	N/C		
6	N/C		

7.15.2 Intrusion Cable Connector

Table 95. Intrusion Cable Connector (J19) Pin-out

Pin	Signal Name
1	INTRUDER_N
2	GND

7.15.3 SCSI LED Header

Table 96. SCSI LED Header Pin-out (J26)

Pin	Signal Name	Description
1	GND	Ground
2	SCSI_CONN_LED_N	Activity Signal
3	SCSI_CONN_LED_N	Activity Signal
4	GND	Ground

7.16 Configuration Jumpers

This section describes the configuration jumpers on the server boards.

7.16.1 System Recovery and Update Jumpers

The server boards provide an 11-pin single inline header (J17), located on the edge of the server board next to PCI Slot 1, this header provides a total of three 3-pin jumper blocks that are used to configure several system recovery and update options. Figure 19 shows the factory default locations for each jumper option.

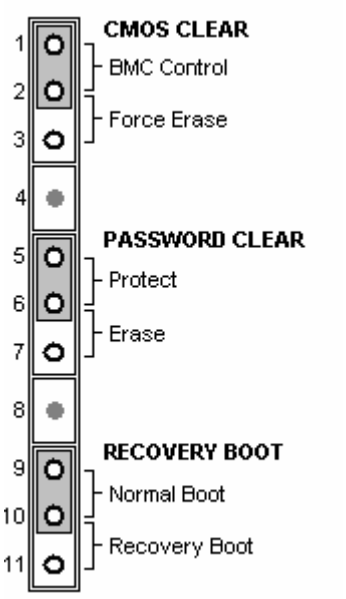


Figure 19. System Configuration Jumpers (J17)

The following table describes each jumper option.

Table 97. Configuration Jumper Options

Option	Description
CMOS Clear	If pins 1 and 2 are jumpered (default), preservation of configuration CMOS through system reset is controlled by the mBMC. If pins 2 and 3 are jumpered, CMOS contents are set to manufacturing default during system reset.
Password Clear	If pins 1 and 2 are jumpered (default), the current BIOS Setup Utility passwords are maintained during system reset. If pins 2 and 3 are jumpered, the Administrator and user passwords are cleared on reset.
Recovery Boot	If pins 1 and 2 are jumpered (default) the system will attempt to boot using the BIOS programmed in the Flash memory. If pins 2 and 3 are jumpered, the BIOS will attempt a recovery boot, loading BIOS code from a floppy disk into the Flash device. This is typically used when the BIOS code has been corrupted.

7.16.2 Rolling BIOS Bank Selection Jumper

An additional 3-pin jumper header (J26) is provided to support the Rolling BIOS functionality. This jumper is located near the processor 2 VRD heatsink and the SATA connectors on the board. The jumper provides the option to force the board to boot from Bank 0 as part of the Rolling BIOS feature. The figure below shows the factory default location for the jumper option.

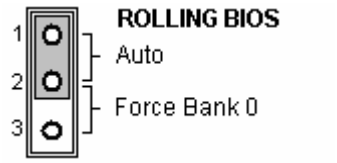


Figure 20. BIOS Bank Jumper (J26)

The following table describes the jumper option.

Table 98. BIOS Bank Jumper Option

Option	Description
Auto	If pins 1 and 2 are jumpered (default), the platform instrumentation on the board controls which BIOS bank has the BIOS the board is intended to boot from.
Force Bank0	If pins 2 and 3 are jumpered, the server board is forced to boot by using the BIOS code stored in Bank0.

8. General Specifications

8.1 Absolute Maximum Ratings

Operating either server board at conditions beyond those shown in the following table may cause permanent damage to the system. The table is provided for stress testing purposes only. Exposure to absolute maximum rating conditions for extended periods may affect system reliability.

Table 99. Absolute Maximum Ratings

Operating Temperature	0 degrees C to 55 degrees C
Non-operating Temperature	-40 degrees C to +70 degrees C
Voltage on any signal with respect to ground	-0.3 V to Vdd + 0.3V
3.3 V Supply Voltage with Respect to ground	-0.3 V to 3.63 V
5 V Supply Voltage with Respect to ground	-0.3 V to 5.5 V

Notes:

Chassis design must provide proper airflow to avoid exceeding Intel® Xeon® processor maximum case temperature.

VDD means supply voltage for the device

Note: *Intel Corporation server boards contain a number of high-density VLSI and power delivery components which 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 can not be held responsible, if components fail or the server board does not operate correctly when used outside any of their published operating or non-operating limits.*

8.2 Mean Time Between Failure (MTBF)

Intel has calculated the MTBF for the server boards as follows:

Table 100. MTBF Calculation

Ambient Temperature	MTBF Calculation
55° C	97,164
40° C	108,598

8.3 Processor Power Support

The server boards are designed to support the Thermal Design Point (TDP) guideline for Intel® Xeon® processors. In addition, the Flexible Motherboard Guidelines (FMB) have been followed to help determine the suggested thermal and current design values for anticipating future processor needs. Table 101 provides maximum values for Icc, TDP power and T_{CASE} for the Intel Xeon processor family.

Table 101. Intel® Xeon® Processor DP TDP Guidelines

TDP Power	Max TCASE	Icc MAX
103 W	72º C	92 A

Note: *These values are for reference only. The processor EMTS contains the actual specifications for the processor. If the values found in the EMTS are different then those published here, the EMTS values will supersede these, and should be used.*

8.4 Power Supply Specifications

This section provides power supply design guidelines for an system using either server board, including voltage and current specifications, and power supply on/off sequencing characteristics.

Table 102. Power Supply Voltage Specification

Output	Min	Max	Tolerance
+3.3 V	3.14 V	3.46 V	+5 / -5 %
+5 V	4.75 V	5.25 V	+5 / -5 %
+12 V	11.40 V	12.60 V	+5 / -5%
-12 V	-11.40 V	-13.08 V	+5 / -9 %
+5 V SB	4.75 V	5.25 V	+5/ -5%

8.4.1 Power Timing

This section discusses the timing requirements for operation with a single power supply. The output voltages must rise from 10% to within regulation limits (T_{vout_rise}) within 5 ms to 70 ms. The +3.3 V, +5 V and +12 V output voltages start to rise approximately at the same time. All outputs must rise monotonically. The +5 V output must be greater than the +3.3 V output during any point of the voltage rise, however, never by more than 2.25 V. Each output voltage shall reach regulation within 50 ms (T_{vout_on}) of each other and begin to turn off within 400 ms (T_{vout_off}) of each other.

Figure 21 shows the output voltage timing parameters.

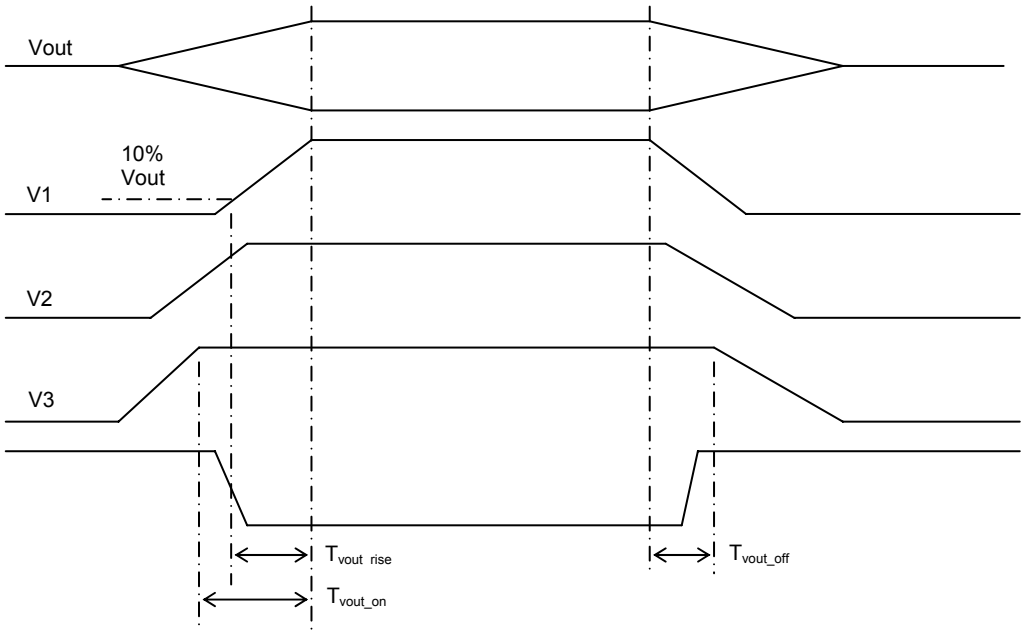


Figure 21. Output Voltage Timing

The following tables show the timing requirements for a single power supply being turned on and off via the AC input, with PSON held low and the PSON signal, with the AC input applied. The ACOK# signal is not being used to enable the turn on timing of the power supply.

Table 103. Voltage Timing Parameters

Item	Description	Min	Max	Units
T_{vout_rise}	Output voltage rise time from each main output.	5	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

Table 104. Turn On / Off Timing

Item	Description	Min	Max	Units
Tsb_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
Tvout_holdup	Time all output voltages stay within regulation after loss of AC.	21		msec
Tpwok_holdup	Delay from loss of AC to de-assertion of PWOK	20		msec
Tpson_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
Tpwok_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	200	msec
Tpwok_low	Duration of PWOK being in the de-asserted state during an off/on cycle using AC or the PSON signal.	100		msec
Tsb_vout	Delay from 5 V SB being in regulation to O/Ps being in regulation at AC turn on.	50	1000	msec
T5vsb_holdup	Time the 5 VSB output voltage stays within regulation after AC lost.	70		msec

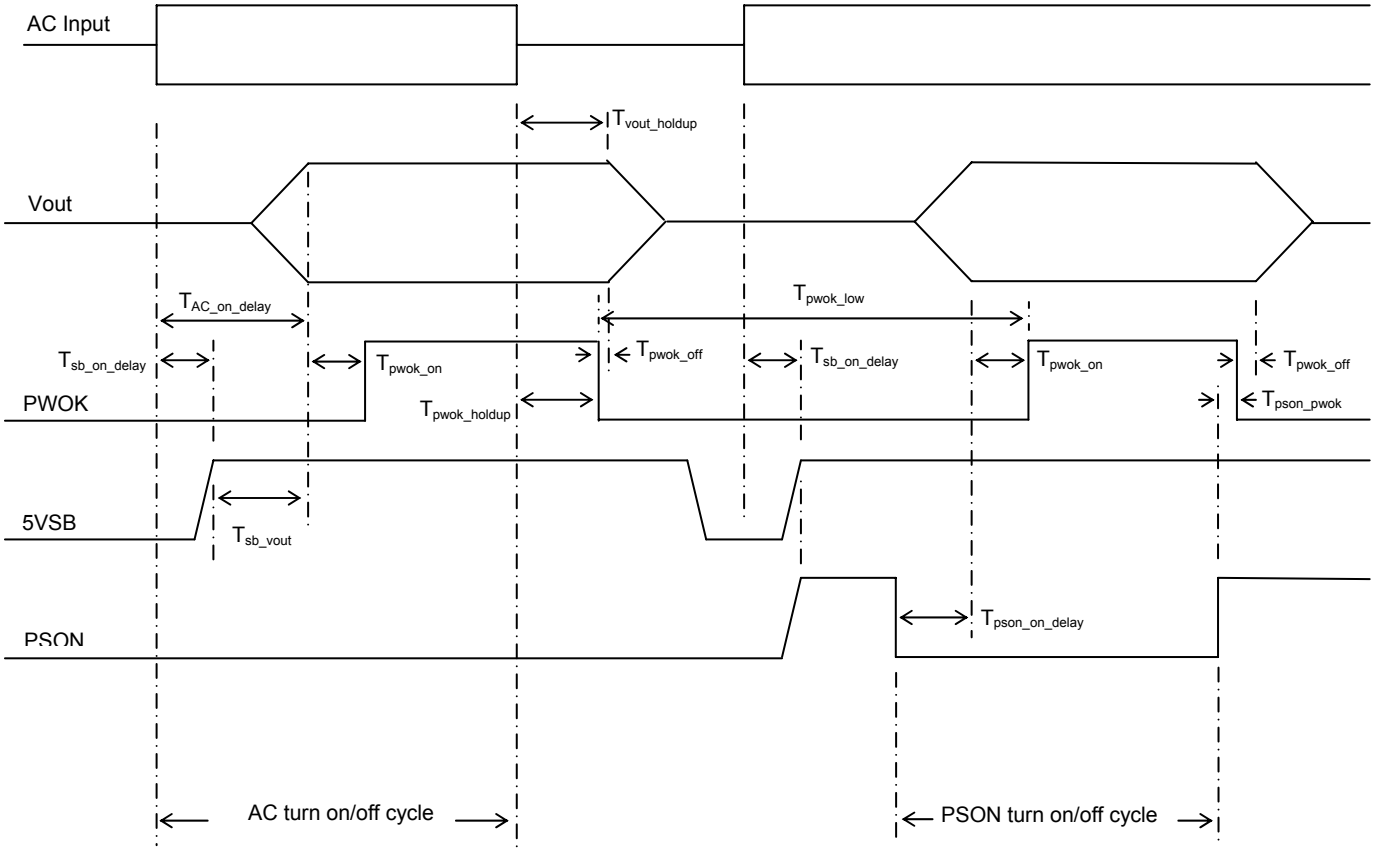


Figure 22. Turn On / Off Timing

8.4.2 Voltage Recovery Timing Specifications

The power supply must conform to the following specifications for voltage recovery timing under load changes:

- Voltage shall remain within +/- 5% of the nominal set voltage on the +5 V, +12 V, 3.3 V, -5 V and -12 V output, during instantaneous changes in load shown in the following table.
- Voltage regulation limits shall be maintained over the entire AC input range and any steady state temperature and operating conditions specified.
- Voltages shall be stable as determined by bode plot and transient response. The combined error of peak overshoot, set point, regulation, and undershoot voltage shall be less than or equal to +/-5% of the output voltage setting. The transient response measurements shall be made with a load changing repetition rate of 50 Hz to 5 kHz. The load slew rate shall not be greater than 0.2 A/ s.

Table 105. Transient Load Requirements

Output	Step Load Size	Load Slew Rate	Capacity Load
+3.3 V	7.0 A	0.25 A/ s	4700 F
+5 V	7.0 A	0.25 A/ s	1000 F
+12 V	6.25 A	0.25 A/ s	675 F
+5 VSB	500 mA	0.25 A/ s	20 F

9. Product Regulatory Compliance

9.1 Product Safety Compliance

The server boards comply with the following safety requirements:

- UL60950 - CSA60950 (US/Canada) - Recognition
- EN 60950 (CENELEC Europe)
- IEC60950 (International)
- CE – Low Voltage Directive 73/23/EEE (CENELEC Europe)
- CB Certificate and Report, IEC60950 (report to include all country notional deviations)
- GOST R 50377-92 – License (Russia) [1]
- Belarus License (Belarus) [1]

***Note**: Certifications for boards in Russia and Belarus are not legal requirements, however, for ease of importing, boards into these countries the boards must be list on System Level GOST license. Alternatively you can obtain voluntary GOST certification for the board.*

9.1.1 Product EMC Compliance

The server boards have been tested and verified to comply with the following electromagnetic compatibility (EMC) regulations when installed in a compatible Intel host system. For information on compatible host system(s), contact your local Intel representative.

- FCC/ICES-003 Verification to Class A Emissions (USA/Canada)
- CISPR 22 - Class A Emissions (International)
- EN55022 - Class A Emissions (CENELEC Europe)
- EN55024 Immunity (CENELEC Europe)
- CE – EMC Directive 89/336/EEC) (CENELEC Europe)
- VCCI Class A Emissions (Japan) – Verify Compliance Only
- AS/NZS 3548 Class A Emissions (Australia / New Zealand)
- BSMI CNS13438 Class A Emissions (Taiwan) – DOC
- GOST R 29216-91 Class A Emissions (Russia) [1]
- GOST R 50628-95 Immunity (Russia) [1]
- RRL MIC Notice No. 1997-41 (EMC) and 1997-42 (EMI) (Korea)

***Note**: Certifications for boards in Russia and Belarus are not legal requirements, however, for ease of importing, boards into these countries the boards must be list on System Level GOST license. Alternatively you can obtain voluntary GOST certification for the board.*

9.1.2 Mandatory/Standard: Certifications, Registration, Declarations

- UL Recognition (US/Canada)
- CE Declaration of Conformity (CENELEC Europe)
- FCC/ICES-003 Class A Verification (USA/Canada)
- VCCI Certification (Japan) – Verification Only
- C-Tick Declaration of Conformity (Australia)
- MOC Declaration of Conformity (New Zealand)
- BSMI Certification (Taiwan)
- GOST R Certification/License (Russia) [1]
- Belarus Certification/License (Russia) [1]
- RRL Certification (Korea)
- ECMA TR/70 Declaration (International)

***Note**: Certifications for boards in Russia and Belarus are not legal requirements, however, for ease of importing, boards into these countries the boards must be list on System Level GOST license. Alternatively you can obtain voluntary GOST certification for the board.*

9.1.3 Product Regulatory Compliance Markings

This product is provided with the following Product Certification Markings.

- cURus Recognition Mark
- CE Mark
- Russian GOST Mark
- Australian C-Tick Mark
- Korean RRL MIC Mark
- Taiwan BSMI Certification Number R33025 and BSMI EMC Warning

9.2 Electromagnetic Compatibility Notices

9.2.1 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.

9.2.2 Australian Communications Authority (ACA) (C-Tick Declaration of Conformity)

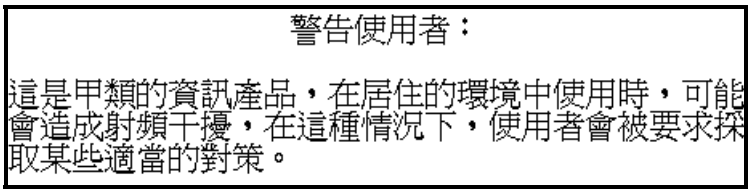
This product has been tested to AS/NZS 3548, and complies with ACA emission requirements. The product has been marked with the C-Tick Mark to illustrate its compliance.

9.2.3 Ministry of Economic Development (New Zealand) Declaration of Conformity

This product has been tested to AS/NZS 3548, and complies with New Zealand's Ministry of Economic Development emission requirements.

9.2.4 BSMI (Taiwan)

The BSMI Certification number R33025 is silk screened on the component side of the server board; and the following BSMI EMC warning is located on solder side of the server board.



9.3 Replacing the Back up Battery

The lithium battery on the server board powers the real time clock (RTC) for up to 10 years in the absence of power. When the battery starts to weaken, it loses voltage, and the server settings stored in CMOS RAM in the RTC (for example, the date and time) may be wrong. Contact your customer service representative or dealer for a list of approved devices.

WARNING
Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the equipment manufacturer. Discard used batteries according to manufacturer's instructions.

ADVARSEL!
Lithiumbatteri - Eksplosionsfare ved fejlagtig håndtering. Udskiftning må kun ske med batteri af samme fabrikat og type. Levér det brugte batteri tilbage til leverandøren.

ADVARSEL
Lithiumbatteri - Eksplosjonsfare. Ved utskifting benyttes kun batteri som anbefalt av apparatfabrikanten. Brukt batteri returneres apparatleverandøren.

VARNING
Explosionsfara vid felaktigt batteribyte. Använd samma batterityp eller en ekvivalent typ som rekommenderas av apparattillverkaren. Kassera använt batteri enligt fabrikantens instruktion.

VAROITUS
Paristo voi räjähtää, jos se on virheellisesti asennettu. Vaihda paristo ainoastaan laitevalmistajan suosittelemaan tyyppiin. Hävitä käytetty paristo valmistajan ohjeiden mukaisesti.

Appendix A: Integration and Usage Tips

This section provides a bullet list of useful information that is unique to the Intel® Server Boards SE7320SP2 and SE7525GP2 and should be kept in mind while assembling and configuring a system based on either of these boards.

- Only Intel® Xeon® processors designed to operate on the 800MHz system bus are supported. Intel® server boards SE7320SP2 and SE7525GP2 are not designed for multi-core processor.
- Processors must be populated in sequential order; socket CPU1 must be populated before socket CPU 2.
- You do not need to install a terminator in an unused processor socket.
- Only DDR 266 or 333 MHz SDRAM memory is supported. Memory installation occurs in pairs of contiguous sockets (e.g. DIMM 1A and DIMM 1B). Within each pair, the DIMMs need to be the same size and vendor. DIMM pair 1 is located furthest from the MCH.
- When integrating Intel® Server Boards SE7320SP2 or SE7525GP2 into the Intel® Server Chassis SC5300 or the Intel® Entry Server Chassis SC5275-E, users will be required to install additional standoffs in the chassis base plate. See the server board *Quick Start User's Guide* for details.
- Intel® Server Boards SE7320SP2 and SE7525GP2 enable six system fan headers: Sys Fan 1 through Sys Fan 6. Sys Fan 5 and Sys Fan 6 are used when integrating the server board in the Intel® Server Chassis SC5300 Base. Sys Fan 2 and Sys Fan 3 are used when integrating the server board in the Intel® Entry Server Chassis SC5275-E.
- When integrating Intel® Server Boards SE7320SP2 or SE7525GP2 into the Intel® Server Chassis SC5300, the system utilizes the 2U passive (no fan) heatsink solution of the Intel® Xeon® processor. If you are integrating either of these server boards into the Intel Entry Server Chassis SC5275-E, the system will utilize the 2U active (with fan) heatsink.
- When integrating Intel® Server Boards SE7320SP2 or SE7525GP2 into a third-party chassis, configure the system fan and processor heatsink as indicated for the Intel® Entry Server Chassis SC5275-E and the Intel® Server Chassis SC5300 Base. These will have adequate load of current on 12V during power-on to meet the minimum loading spec of the power supply.
- When integrating Intel® Server Boards SE7320SP2 or SE7525GP2 into the Intel® Server Chassis SC5300, ensure the rubber “L” gasket is installed under the server board prior to mounting the server board to the base plate. Thermals will be adversely affected without this gasket in place. See the *Quick Start User’s Guide* for details on where the gasket is affixed.
- When setting up the boot order sequence in the BIOS setup, keep in mind that any time one of the devices in the boot menu is modified or removed, the BIOS will reset the boot sequence. The user will need to ensure they enter the BIOS setup and restore the boot order they desire any time a change is made to a controller (i.e. enter the option ROM and make a configuration change) or a controller is removed from the system.

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.

Word / Acronym	Definition
ACPI	Advanced Configuration and Power Interface
BMC	Baseboard Management Controller
CEK	Common Enabling Kit
CME	Correctable Memory Error
DVI	Digital Video Interface
FML	Fast Management Link
FMM	Flexible Management Module
FSB	Front Side Bus
KCS	Keyboard Controller Style
LPC	Low Pin Count
mBMC	Mini Baseboard Management Controller
MCH	Memory Controller Hub
NMI	Non-maskable Interrupt
PATA	Parallel ATA
PCB	Printed Circuit Board
PWM	Pulse Width Modulation
RTC	Real-time Clock
SATA	Serial ATA
SIO	Super Input/Output (I/O)
SM	System Management
SMC	System Management Controller
USB	Universal Serial Bus
VRD	Voltage Regulator Down