Bull NovaScale 4020

User's Guide

Bull NovaScale 4020

User's Guide

Software

February 2004

Trademarks and Acknowledgements

We acknowledge the right of proprietors of trademarks mentioned in this book.

Intel® and Itanium® are registered trademarks of Intel Corporation.

Windows® and Microsoft® software are registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark in the United States of America and other countries licensed exclusively through the Open Group.

Linux® is a registered trademark of Linus Torvalds.

Important Safety Information

Read all caution and safety statements at the end of this document before performing any of the instructions.

⚠ WARNING

If the server is rack-mounted, follow the instructions hereafter: The equipment rack must be anchored to an unmovable support to prevent it from falling over when one or more servers are extended in front of the rack on slides. The anchors must be able to withstand a force of up to 113 kg (250 lbs.). You must also consider the weight of any other device installed in the rack. A crush hazard exists should the rack tilt forward which could cause serious injury.

Main AC power disconnects: You are responsible for installing an AC power disconnect for the entire rack unit. This main disconnect must be readily accessible, and it must be labeled as controlling power to the entire unit, not just to the server(s).

Grounding the rack installation: To avoid the potential for an electrical shock hazard, you must include a third wire safety-grounding conductor with the rack installation. If the server power cord is plugged into an AC outlet that is part of the rack, then you must provide proper grounding for the rack itself. If the server power cord is plugged into a wall AC outlet, the safety-grounding conductor in the power cord provides proper grounding only for the server. You must provide additional, proper grounding for the rack and other devices installed in it.

Overcurrent protection: The server is designed for an AC line voltage source with up to 20 amperes of overcurrent protection. If the power system for the equipment rack is installed on a branch circuit with more than 20 amperes of protection, you must provide supplemental protection for the server.

⚠ WARNING – POWER CORD RATING

Do not attempt to modify or use an AC power cord that is not the exact type required. You must use a power cord that meets the following criteria:

a. Rating: For U.S./Canada cords must be UL Listed/CSA Certified, 16/3, 75C type, VW-1, SJT/SVT, with NEMA 5-15P or NEMA 6-15P attachment plug and IEC 320 C13 input power connector rated 15 amps. For outside U.S./Canada cords must be flexible harmonized (<HAR>) rated 250 V, 1.0 mm minimum conductor size with IEC 320 C13 input power connector and rated for no less than 10 amps.

b. Input Power Connector, server end: The connectors that plug into the AC receptacles on the server must be an IEC 320, sheet C13, type female connector and are rated for 125 V/250 V, 15 A.

c. **Cord length and flexibility: Cords must be less than 4.5 meters (14.76 feet) long.**

If the Server is rack-mounted, the Server power units must be connected to the Power Distribution Unit (PDU) located at the back of the Cabinet. Use the power cords provided with the PDU. Connect the power cord to the outlet in the front of the PDU. DO NOT use the outlets at the rear of the PDU.

⚠ CAUTION

Temperature: The range of temperatures in which the server operates when installed in an equipment rack, must not go below 10 °C (50 °F) or rise above 35 °C (95 °F). Extreme fluctuations in temperature can cause a variety of problems in your server.

Ventilation: The equipment rack must provide sufficient airflow to the front of the server to maintain proper cooling. The rack must also include ventilation sufficient to exhaust a maximum of 650 W (2,300 BTU/hr) for the server. The rack selected and the ventilation provided must be suitable to the environment in which the server will be used.

Regulatory Specifications and Disclaimers

Declaration of the Manufacturer or Importer

We hereby certify that this product is in compliance with European Union EMC Directive 89/336/EEC, using standards EN55022 (Class A) and EN55024 and Low Voltage Directive 73/23/EEC, using standard EN60950. The product has been marked with the CE Mark to illustrate its compliance.

Safety Compliance

USA	UL 1950 – 3rd Edition/CSA 22.2. No. 950-M93
Canada	UL certified – 3rd Edition/CSA 22.2. No. 950-M93 for Canada (product bears the single UL mark for U.S. and Canada)
Europe	Low Voltage Directive, 73/23/EECTUV/GS to EN60950 2nd Edition with Amendments, A1 = A2 + A3 + A4
International	TUV/CB to IEC 60950 3rd Edition TUV/CB - EN60 950 2nd Edition + Amendment 1-4TUV/CB - EMKO-TSE (74-SEC) 207/94 plus international deviations
Australian / New Zealand	CB Report to IEC 60950, 3rd Edition plus Australian deviations

Electromagnetic Compatibility (EMC)

USA:	FCC CFR 47 Part 2 and 15, Verified Class A Limit
Canada:	IC ICES-003 Class A Limit
Europe:	EMC Directive, 89/336/EEC • · EN55022, Class A Limit, Radiated & Conducted Emissions • · EN55024, ITE Specific Immunity Standard • · EN61000-4-2, ESD Immunity (Level 2 Contact Discharge, Level 3 Air Discharge) • · EN61000-4-3, Radiated Immunity (Level 2) • · EN61000-4-4, Electrical Fast Transient (Level 2) • · EN61000-4-5, AC Surge • · EN61000-4-6, Conducted RF • · EN61000-4-8, Power Frequency Magnetic Fields • · EN61000-4-11, Voltage Dips and Interrupts • · EN61000-3-2, Limit for Harmonic Current Emissions • · EN61000-3-3, Voltage Flicker
Japan:	VCCI Class A ITE (CISPR 22, Class A Limit) IEC 1000-3-2 Limit for Harmonic Current Emissions
Australia/New Zealand:	AS/NZS 3548, Class A
Taiwan:	BSMI Approval, Class A
Korea:	RRL Approval, Class A
Russia:	GOST Approved
International:	CISPR 22, Class A Limit

Federal Communications Commission (FCC) Statement

☞ **Note:**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Neither the provider nor the manufacturer are responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

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

FCC Declaration of Conformity

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

Laser Compliance Notice

This product that uses laser technology complies with Class 1 laser requirements.

A CLASS 1 LASER PRODUCT label is located on the laser device.

Class 1 Laser Product
Luokan 1 Laserlaite
Klasse 1 Laser Apparat
Laser Klasse 1

Japan EMC Compatibility

> この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

English translation of the notice above:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

ICES-003 (Canada)

> Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: «Appareils Numériques», NMB-003 édictée par le Ministre Canadian des Communications.

English translation of the notice above:

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

Conventions

The following conventions are used in this manual:

⚠ WARNING

> **Warnings indicate conditions that, if not observed, can cause personal injury.**

⚠ CAUTION

> Cautions warn you about how to prevent damage to hardware or loss of data.

📝 NOTE

> Notes call attention to important information.

Contents

Figures

Tables

1 System Description

The NovaScale 4020 Server is a compact, high-density, rack mount server system with support for one to two Intel® Itanium® 2 processors and 16-GB DDR SDRAM memory. The scaleable architecture of the system supports Symmetric Multiprocessing (SMP) and a variety of operating systems.

The server system supports several high availability features, such as hot-swap and redundant power supply modules, hot-swap and redundant fans for cooling, and hot-swap hard drives. Serviceability features include LED indicators for system, reset, hard drive and LAN status and system identification. Additional features include video connector and dual USB ports accessible from the front panel. Color-coded parts differentiate hot-swap and non-hot-swap serviceable components.

Figure 1 provides a diagram of the front and top of the server system, with the chassis cover in place.
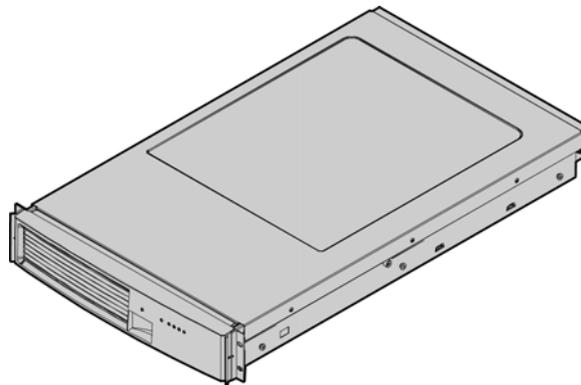
Figure 1. Server System Front

Table 1 provides the system dimensions and weight.

Table 1.   Physical Specifications

Specification	Value
Height	3.4 inches (87 mm)
Width	17.7 inches (449 mm)
Depth	29.4 inches (747 mm)
Front clearance	3 inches (76 mm)
Side clearance	1 inch (25 mm)
Rear clearance	6 inches (152 mm)
Weight (note 1)	65 lbs (30 kg)
Heat dissipation	650 W (2,300 BTUs)

Note 1.   The system weight listed above is an estimate for a fully configured system and will vary depending on the number of peripheral devices and add-in cards as well as the number of processors and DIMMs installed in the system.

Table 2 provides a list and brief description of the features of the server system.

Table 2.   Feature Summary

Feature	Description	
Compact, high-density system	Rack-mount server with a height of 2U (3 1/2 inches) and a depth of 28 inches	
Configuration flexibility	• 1-2 way capability in low profile and cost effective packaging • Stand-alone system including external I/O slots/disk expansion as needs grow • Intel Itanium 2 processor support • 16-GB Double Data Rate (DDR) Synchronous Dynamic Random Access Memory (SDRAM) memory support	
Serviceability	• Front access to hot-swap hard drives • Hot-swap fans • Front access to hot-swap power supplies • Dockable power to main board • System power and reset status LEDs • System ID switch on front panel and LEDs on front and back • Color-coded parts to identify hot-swap and non-hot-swap serviceable components	
Availability	• Three PCI-X slots • Three hot-swap 350-W power supplies in a redundant (2+1) configuration • Dual redundant power cords (1+1) when three power supplies are present • Six hot-swap system fans in a redundant (5+1) configuration • Two hot-swap 1-inch Ultra320 SCSI hard drives	
Manageability	• Remote management • Emergency Management Port (EMP) • Intelligent Platform Management Interface (IPMI) 1.5 compliant • Wired For Management (WfM) 2.0 compliant • Remote diagnostics support	
Upgradeability and investment protection	• Supports Intel Itanium 2 processors • Field upgradeable to next generation (Montecito) processor family • Multi-generational chassis	
System-level scalability	• Up to 16-GB DDR SDRAM (using 2-GB DIMMs) • One to two Intel Itanium 2 processors • External I/O (3 slots) / disk expansion • External SCSI connector	
Front panel	• System Power switch and LED • System Reset switch • System Diagnostic Interrupt (SDINT) switch • System ID switch and LED	• System Status LED • Hard Drive Fault LED • LAN1 & LAN2 Status LEDs • Video Connector • Dual USB 1.1 Ports
Removable media	• DVD/CDRW • External USB floppy or key fob	

External Chassis Features

System controls and indicators are located in several places on the chassis as follows:

- Chassis front:
  - Front panel: Front panel switches and LEDs
  - Peripheral bay: Hard drive LEDs
  - Power bay: Power Module LEDs and Power Supply LEDs
- Chassis back panel: System ID LEDs and LAN port LEDs

Each of these areas is discussed below.

Chassis Front

The following figure shows the front of the chassis with the snap-on bezel in place. The bezel must be removed to access the front panel switches, power supplies, SCSI drives and DVD-CDRW devices. Figure 3 shows the front of the chassis with the bezel removed.
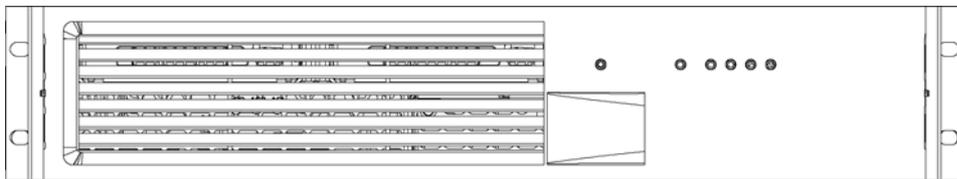
Figure 2. Server System Front with Bezel Installed
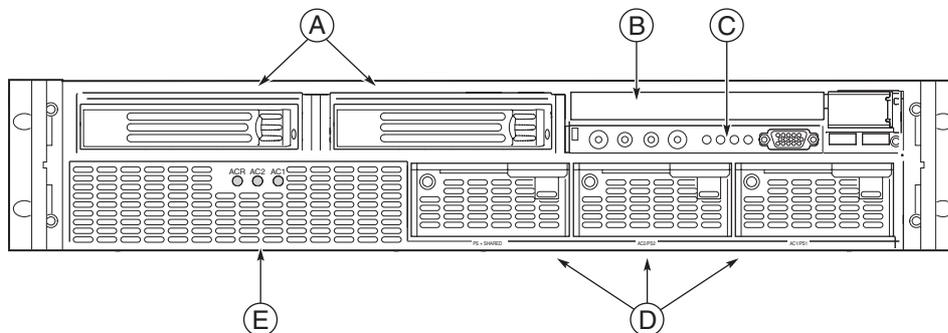
A.	Hard drives	B.	CD-ROM/DVD-ROM drive
C.	Front panel	D.	Power supply modules
E.	Power bay	F.	

Figure 3. Server System Front with Bezel Removed

Front Panel

The front panel is located at the right side of the server system, at the front of the chassis. The front control panel of the displays status lights for system status, hard drives, and power supplies.
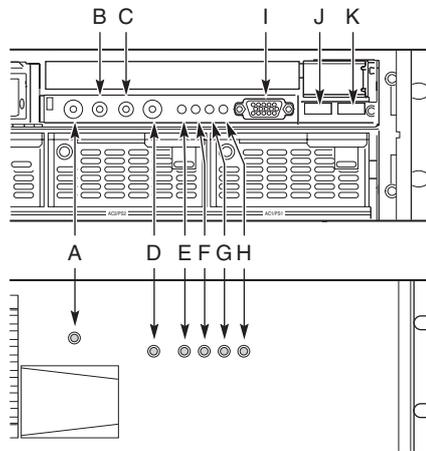
TP00302

Callout	Control, Connector, Indicator	Description
A	System Power switch & LED	Toggles system power **LED** **State** **ACPI** Off Power off No On Power on No Off S5 Yes On S0 Yes
B	System Reset switch	Resets the system.
C	SDINT (System Diagnostic Interrupt) switch	Asserts SDINT
D	System ID switch and LED (Blue)	System identification switch and light
E	System Status/Fault LED (Green/Amber)	Indicates system status. **LED** **State** **Description** Off Not ready Post err/NMI Ev/CPU missing Green, solid Ready No Alarms Green, blinking Ready – Degraded CPU Fault, DIMM killed Amber, solid Critical Alarm Critical of Pwr Flt, Fan, Voltage, and Temperature failures. Amber, blinking Non-Critical Alarm Non-Critical of redundant Pwr Flt, redundant Fan, Voltage, and Temperature failures.

F	Hard Drive Fault LED (Amber)	Indicates hard drive subsystem fault status.		
		LED	**State**	**Description**
		Off	Drive Missing	Slot Empty, Online, Prepare for removal.
		On	Inactive	Drive Failed
		Blinking		Drive Identity, Rebuild, Predictive Fail, Rebuild Interrupt or Rebuild on empty slot.
G, H	LAN1, LAN2 Status LEDs (Green)	Indicates LAN activity status.		
		LED	**State**	**Description**
		Off	Idle	
		On	Inactive	No Access
		Blinking	Active	Access
I	Video connector	Video port, standard VGA compatible, 15-pin connector		
J	USB3 connector	USB port 3, 4-pin connector		
K	USB4 connector	USB port 2, 4-pin connector		

Figure 4. Front Panel Controls, Indicators, and Connectors

Peripheral Bay

The peripheral bay supports up to two 1-inch hot-swap Ultra320 SCSI hard drives and one ½-inch ATA-33 IDE DVD/CD-ROM drive.

The peripheral bay supports Low Voltage Differential (LVD) SCSI disk drives only. Single-Ended (SE) SCSI devices are not supported in the peripheral bay, however SE device support is available via the secondary external SCSI channel located at the rear of the chassis.
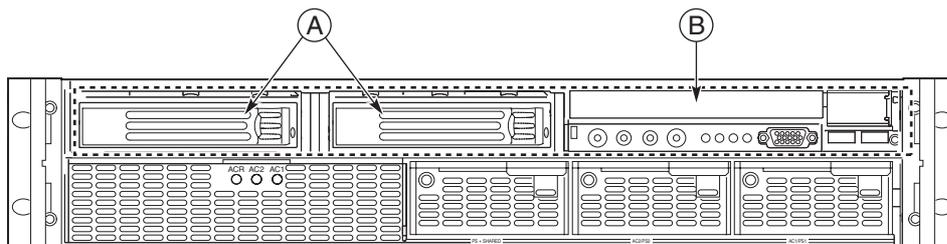
TP00296

A.   Hard drives
B.   CD-ROM/DVD-ROM drive

Figure 5. Peripheral Bay

Hot-swap Hard Drive Carrier

The hot-swap hard drive carrier accepts 15,000-RPM and slower Ultra320 SCSI technology SCA-type hard drives. The peripheral bay supports Low Voltage Differential (LVD) SCSI disk drives only. Single-Ended (SE) SCSI devices are not supported in the peripheral bay. SE drives are only supported on the external SCSI connector. Hard drive carriers that accommodate 3.5-inch by 1.0-inch SCSI disk drives are required as part of the hot-swap implementation. The disk drive is attached to the carrier with four fasteners, and is retained in the chassis by a locking handle. Figure 6 shows a hard drive carrier that has been removed from the peripheral bay. The drive is accessed by pressing the latch to release the drive carrier door, then pulling out on the door.

The SCSI backplane board contains a dual-color LED for each hard drive. The LED can be seen at the right edge of the carrier, as shown in the figure. The LED displays the drive status, as described in Table 3.

A.   LED
B.   Latch
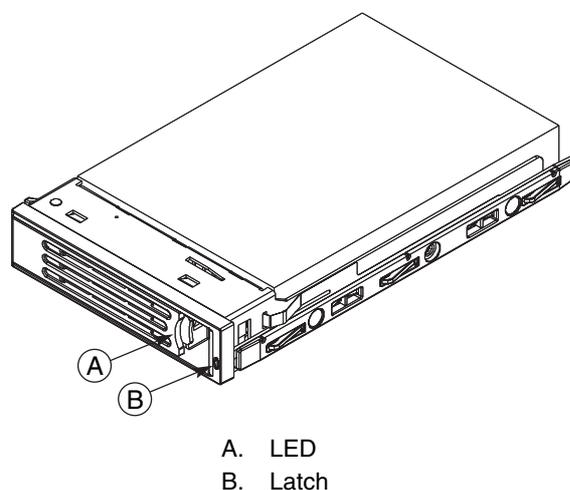
Figure 6. Hard Drive Carrier

Table 3.   SCSI Hard Drive LED Details

Feature	Description
Green, flashing	Indicates the hard drive is active
Yellow/Green flashing	Indicates a hard drive fault and hard drive is powered
Yellow/Blank flashing	Indicates a hard drive fault and hard drive is not powered
Not illuminated	Indicates no hard drive is installed in the bay

Removable Media Drive Bay

⚠ **CAUTION**

> The DVD/CD-ROM drive cannot be hot-swapped. In order to add,
> remove or replace a DVD/CD-ROM drive, the system must be powered
> down, power sources unplugged and the top cover of the chassis must be
> removed to access the DVD/CD-ROM drive area.

The slim-line DVD/CD-ROM drive is installed in a drive carrier that is inserted from the rear of the peripheral bay. This device is not hot-swappable; you must switch off system power, remove all power cords, open the chassis and then remove the peripheral bay to remove or install a CD-ROM or DVD-ROM drive.

The CD-ROM/DVD-ROM drive snaps into the carrier as shown below and is secured by four raised points. The raised points line up with the mounting holes on the sides of the drive. Two of these mounting points are spring loaded and two are stationary.
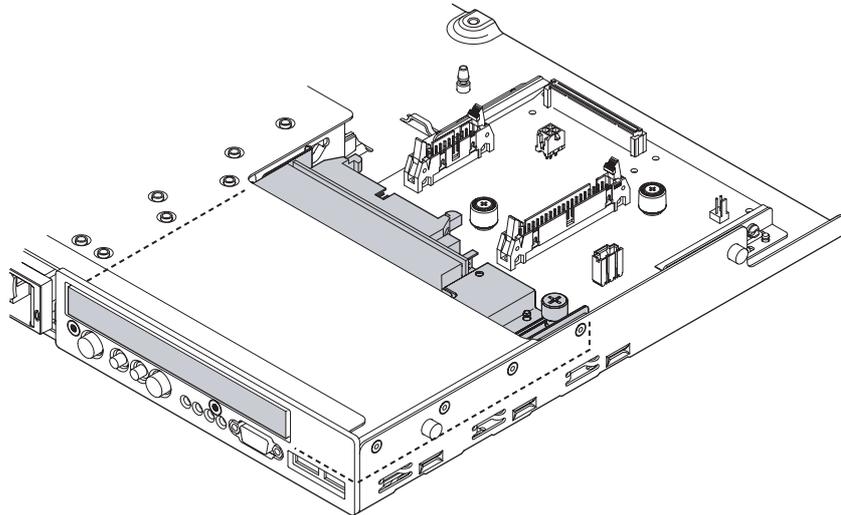
TP00303

Figure 7. DVD-ROM / CD-ROM Drive

Power Supply Bay

The power supply bay, shown below, is located in the lower front of the system. Redundant power status LED indicators are in the left portion of the power bay and three hot-swap power supply modules dock into the three bays on the right.
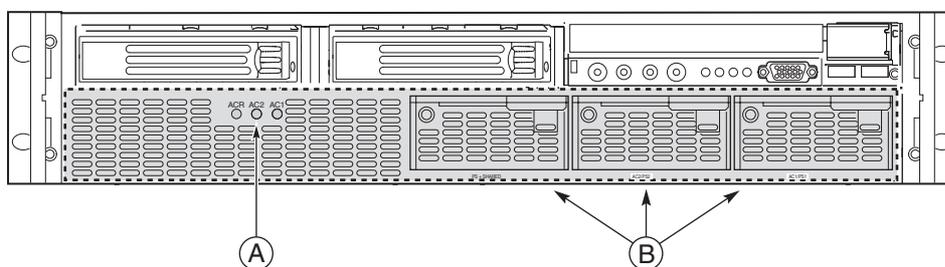
TP00295

A. Power status LEDs
B. Power supply modules

Figure 8. Power Supply Bay

The power subsystem can be configured as follows:
- Three power supply modules installed, (2+1) redundancy
- Two power supply modules installed, non-redundant

NOTE

The power supply modules must be populated from right to left. The left power supply module is optional in a non-redundant configuration. If no module is installed in the left slot, a filler panel is required for proper system cooling.

Two power supply modules are capable of handling the worst-case power requirements for a fully configured server system. This includes two Intel Itanium 2 processors, 16 GB of memory, three PCI add-in cards, two hard drives, and a DVD-ROM / CD-ROM drive.

When the system is configured with three power supply modules, the hot-swap feature allows you to replace a failed power supply module while the system is running.

The power subsystem receives AC power through two power cords. When three power supply modules and two power cords are installed, the system supports (1+1) power cord redundancy. This feature allows the system to be powered by two separate AC sources. In this configuration, the system will continue to function without interruption if one of the AC sources fails.

The AC power status LEDs in the power supply module provide information on the status of the power sources. The LEDs are shown below, indicated by the letter "A" in the diagram. The possible LED states are described below the diagram.
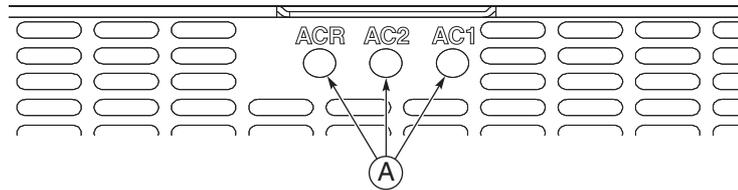
TP00304

LED	Description
AC1 (green)	On - AC input #1 available.
	Off - AC input #1 unavailable or below voltage threshold to power up the system.
AC2 (green)	On - AC input #2 available.
	Off - AC input #2 unavailable or below voltage threshold to power up the system.
ACR (green)	On - redundant feature is available.
	Off - redundant feature is not available

Figure 9. AC Power Status LEDs

The power redundancy feature requires each of the following conditions be present.

- AC input #1 available
- AC input #2 available
- Power good signals asserted from all three power supply modules
- TS-OK signal is asserted

Chassis Rear

The figure below shows the rear of the system.
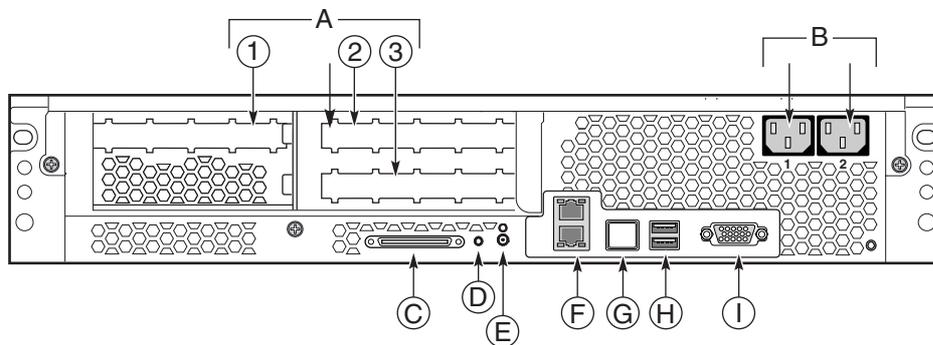
TP00305

Callout	Description	
A	PCI Slots	
	Slot 1	100 MHz, 64-bit PCI-X slot, full length
	Slot 2	100 MHz, 64-bit PCI-X slot, full length
	Slot 3	133 MHz, 64-bit PCI-X slot, full length
B	AC input power connectors (two)	
C	External SCSI connector[1]	
D	System ID switch	
E	System ID LED (blue)	
F	Two LAN ports, RJ45 connector (LAN1 on bottom, LAN2 on top) LAN port LEDs:	
	Status LED (Green)	On – ethernet link is detected
		Off – no ethernet connection
		Blinking – ethernet link is active
	Speed LED (Green/Amber)	Off – 10 Mbps
		Green On – 100 Mbps
		Amber On – 1000 Mbps
G	Serial port[2], RJ45 connector	
H	Two USB 1.1 ports, 4-pin connectors (USB0 on bottom, USB1 on top)	
I	Video port, standard VGA compatible, 15-pin connector	

Notes:

1. External SCSI bus supports both LVDS and SE signals via the external SCSI connector.

2. EMP access is provided via shared serial port.

Figure 10. Chassis Rear Features

Internal Chassis Features

⚠️ **WARNING**

> **Only qualified technical personnel should access any internal system component. Some exposed circuits exceed 240 VA and may cause injury if accidentally contacted.**

Electronics Bay

The electronics bay, shown in the two figures below, consists of the following:

- Main board
- PCI riser board
- Two processor locations and two power pod locations
- Eight DIMM slots
- Air duct for the processor area
- PCI riser bracket to support PCI riser board and PCI cards
- Connectors, switches and LEDs at the rear of the chassis (see
- *Figure* 10)
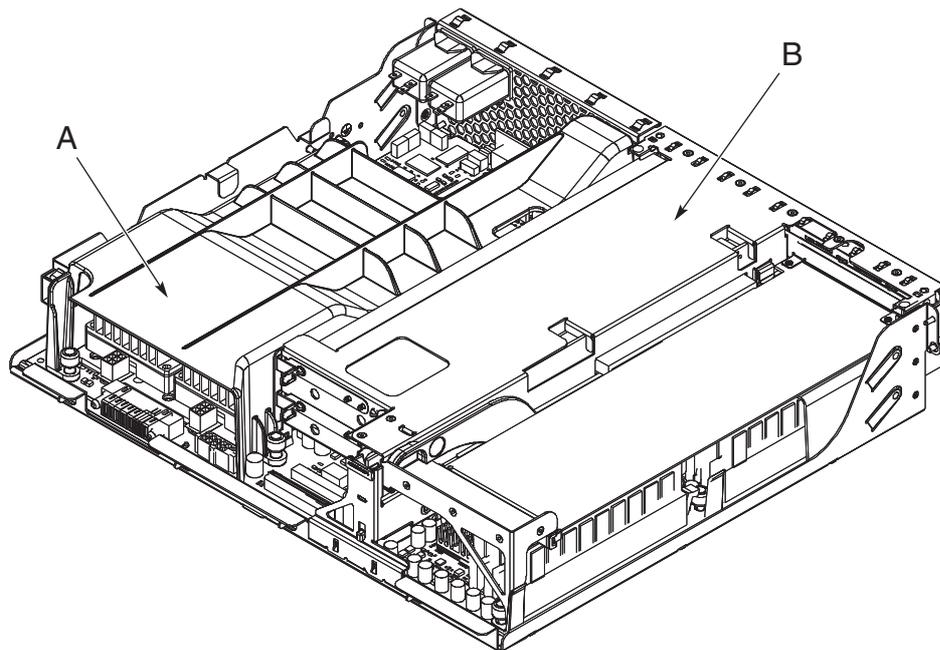
A. Processor air duct with processor(s) installed underneath
B. PCI riser sub-assembly with PCI cards installed

Figure 11. Electronics Bay
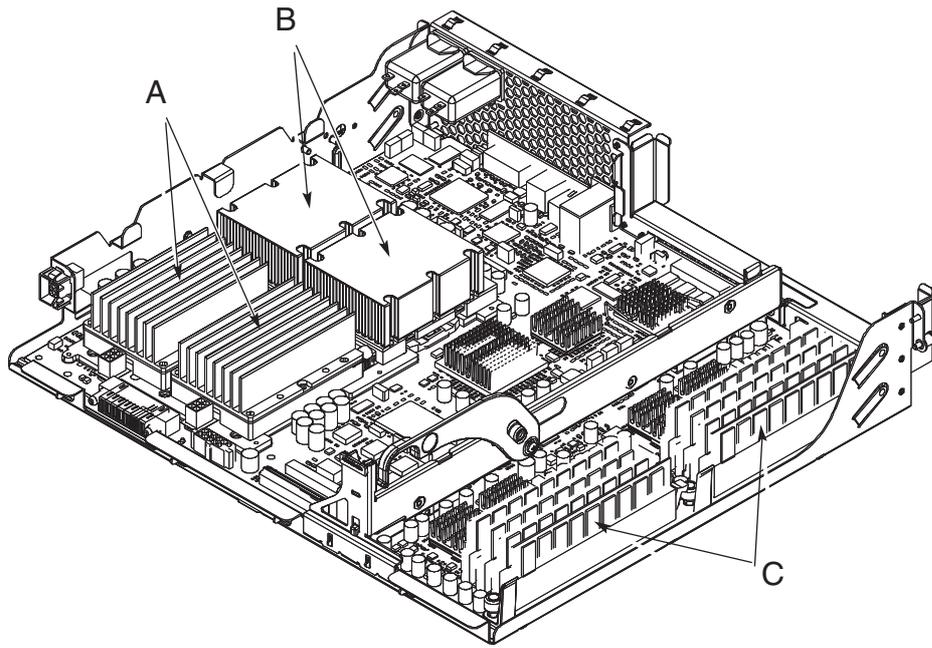
A. Processor pods (2 shown installed)
B. Processors (2 shown installed)
C. DIMMs (8 shown installed)

Figure 12. Electronics Bay (sub-assembly removed)

Cooling Subsystem

⚠ CAUTIONS

The chassis top cover must be installed and closed for proper system cooling.

Cooling components must be hot-swapped within a limited time period. This time period applies only to the time that the cooling component is removed from the system, not from the time of failure.

The cooling subsystem consists of a hot-swap, redundant (5+1) system fan array installed in the fan bay. The single bank of six Delta* FFB0612EHE-S18Z hot-swap system fans provide the airflow necessary to cool the system components. These fans are installed in the fan bay that is located within the power bay. The fans connect to the fan baseboard. The figure below shows the location of the fans in the power bay.
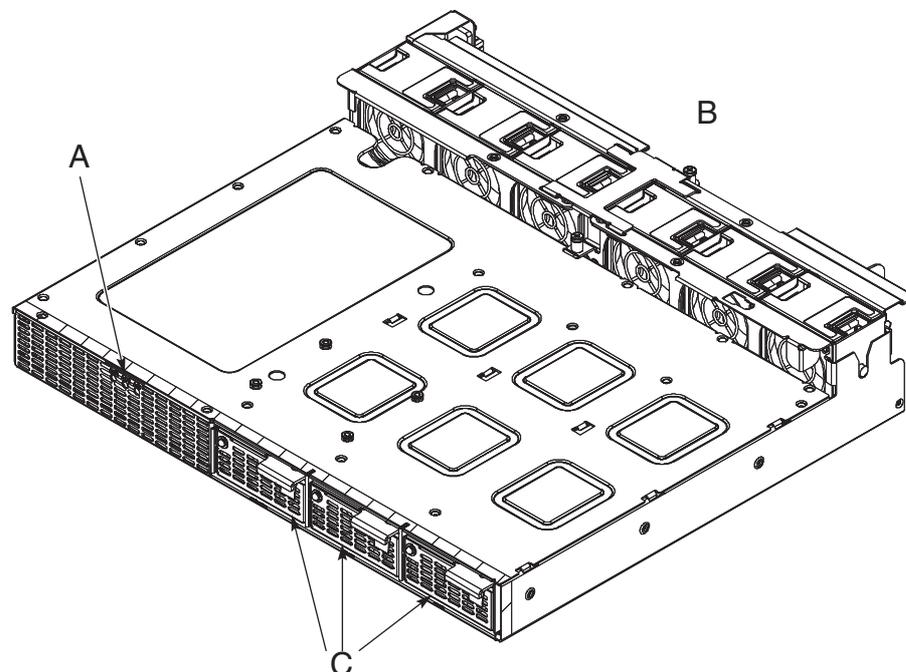
A. AC power status LEDs (three)
B. Fan bay (six installed fans)
C. Power supply modules (three)

Figure 13. Power Bay (removed from chassis)

The figure below shows the cooling subsystem layout with the airflow direction indicated.
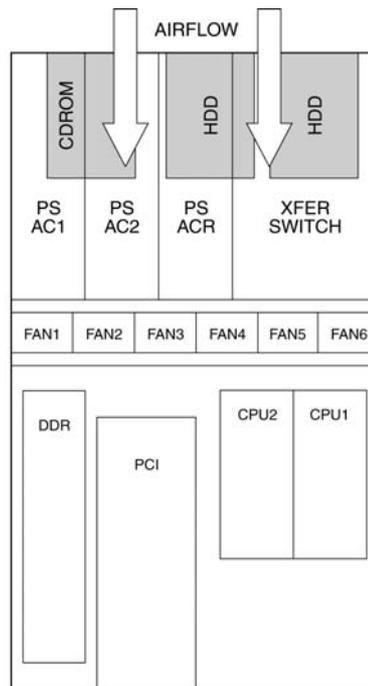
Figure 14. Cooling Subsystem Layout

The server system supports only a fully populated system fan configuration. However, the system will continue to meet thermal specifications with either a system fan or a power supply failure. The power supply redundancy feature applies to systems with three power modules installed.

If a fan fails, system cooling is maintained and the system continues to operate while the failed fan is being hot-swapped. All system fans have tachometer output, internal speed control, and external Pulse Width Modulation (PWM) speed control.

A failure is detected when the RPM of a fan falls below a predetermined minimum threshold (Approx. 5000 RPM). If a system fan falls below this threshold, all fans will be boosted to operate at a higher speed (Approx. 8500 RPM)

The fans will also be boosted to the higher speed if a power supply fails for any reason (including loss of AC power). The fans will not be boosted if the Redundant (ACR) power supply fails. If the redundant power supply fails, the system fans will not be affected.

When boosted, all fans remain at high speed until the failed fan or power supply is replaced. When a fan replacement is detected by a change in state of the fan presence signal. After a failed fan is replaced, the fans return to the lower speed and fan failure monitoring at the lower speed levels is reactivated.

When a power supply fails and is replaced, the replacement is detected by server management.

NOTES

Do not attempt to operate this system with less than a fully populated, six system fan configuration.

To maintain adequate cooling for system components, the swap process must be completed in two-minutes. This period only applies to the time that the fan or power supply is removed from the system, not from the time of failure.

A system fan failure is indicated by the corresponding fan LED and by the Cooling Fault LED on the front panel. The system fan LEDs are shown in the figure below. The LED is amber and turns on if a system fan failure occurs. These LEDs can be seen only when the top cover is removed from the chassis.

TP00310
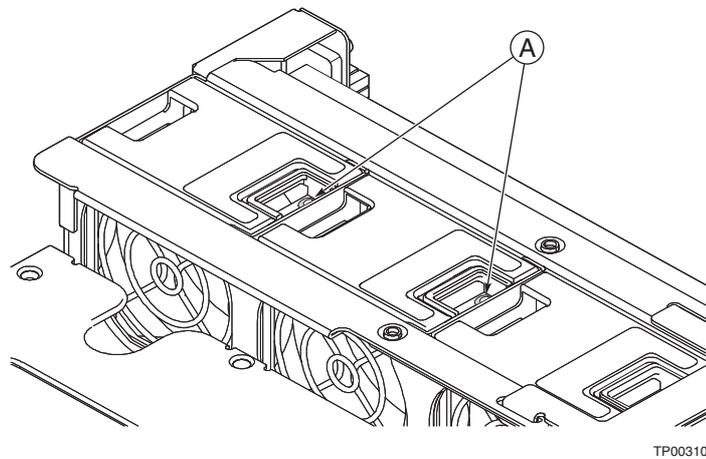
A.   Fan LEDs (two of six pointed out)

Figure 15. System Fan Status LED

Power Subsystem

Power Supply Modules

The power supply modules are Server System Infrastructure (SSI) compliant, universal AC input with Power Factor Correction (PFC) Thin Power Supplies (TPS). The power supply modules are auto-sens over the input range of 200-240 VAC and 100-127 VAC. They are rated at 350 W each. The combined continuous output power for all outputs has been designed such that they will not exceed 650W.

The DC output specification for the power supply is met by two power supply modules operating in the power bay. A third power module can be inserted to enable redundancy. When operated in parallel, the power modules share the total load currents equally within the limits specified, and meet all performance requirements. Two power supply modules are capable of handling the worst-case power requirements for a fully configured system: Two processors, 16 GB of memory, three PCI-X add-in cards, two hard drives and a DVD or CD drive.

In the unlikely event that a power module fails in a redundantly paralleled group, or upon the removal of an operational or failed supply from a redundantly paralleled group, the action will not cause DC output transients in excess of specified limits. Conversely, adding an operational or failed supply to a paralleled group will not cause DC output transients in excess of the limits specified.

Redundant AC Power Source Operation

The power bay has two AC inlets, labeled AC1 and AC2, located at the rear of the chassis. AC1 is connected to the inputs of power supply module PS1. AC2 is connected to module PS2 and the redundant power module PS-Shared, through normally closed transfer switch contacts.

- If AC1 input fails or exceeds the specified voltage range, AC2 will transfer power to the two modules located in the positions labled PS2 and PS-Shared.
- If AC2 input fails, the AC transfer switch automatically switches from AC2 to AC1. As result, AC1 connects to the two power supply modules located in locations PS1 and PS-Shared. After AC2 recovers, the AC transfer switch resets to its original state. This feature allows the system to be powered by two separate AC sources. In this configuration, the system continues to operate without interruption if one of the AC sources fails.

Processor Power Pods

Dedicated power pods supply power to each processor. The input connector of the power pod is connected to the 12 VDC power on the main board via a short 'Y' cable. The output connector of the power pod mates directly with the edge of the processor package.

2 Board Set Description

This chapter highlights the main features of the board set. The board set contains the following:

- Main board
- PCI riser board

In addition, the server contains the following system boards:

- SCSI board
- Front panel board

Major components of the board set include:

- Intel Itanium 2 processors
- Intel® E8870 chip set
- High-capacity DDR SDRAM memory
- High-bandwidth I/O subsystem supporting PCI and PCI-X

The figure on the following page displays a block diagram of the system and the board set within the system.
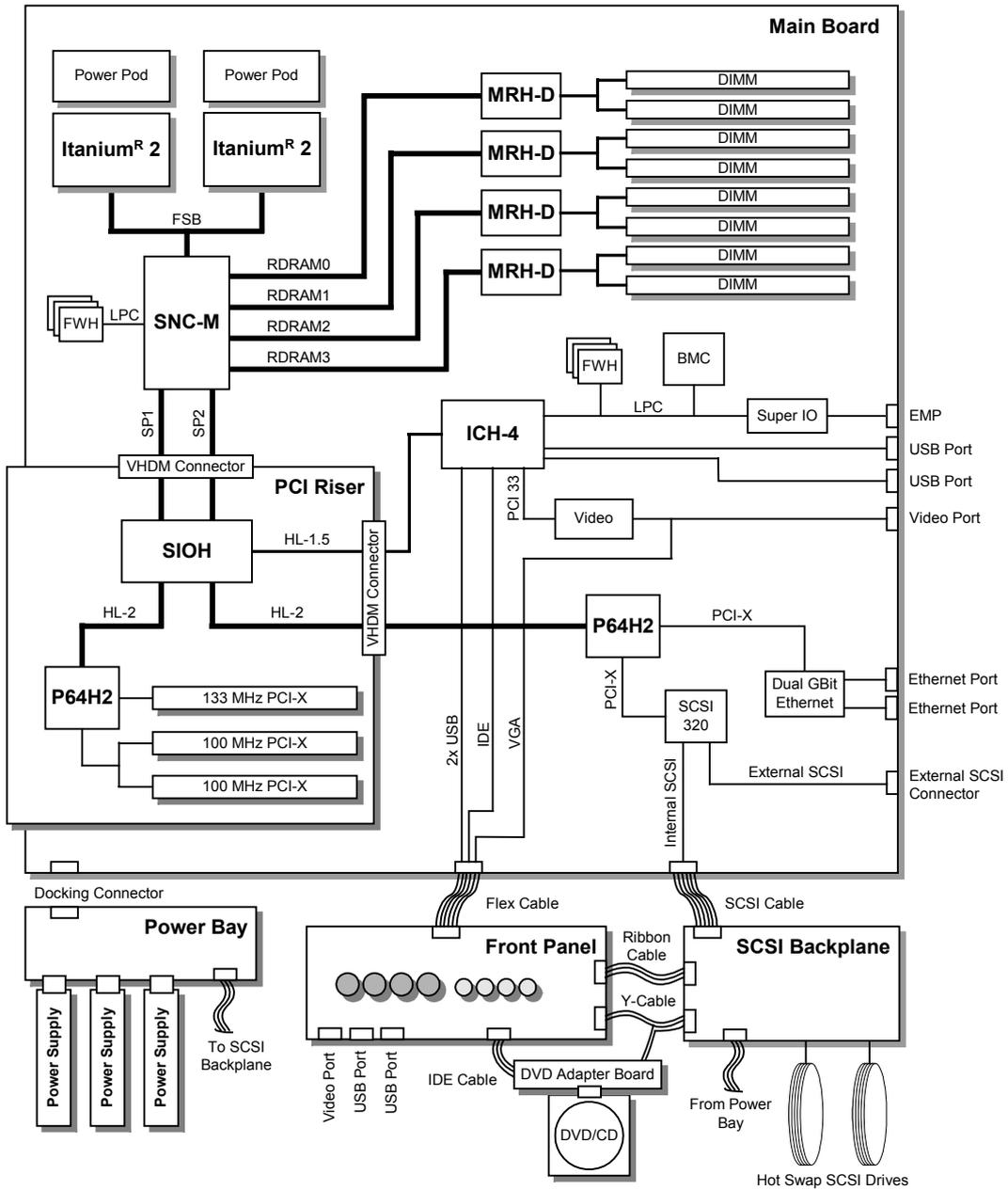
Figure 16. System Architecture Layout

Main Board

The main board connection layout is displayed in *Figure 17*. The main board supports the following features:

- Two Intel Itanium 2 processor sockets and power pod sites
- Eight 184-pin, DDR-SDRAM DIMM sockets
- SNC-M (Scalable Node Controller) of the E8870 chip set
- Four Memory Repeater Hubs – DDR (MRH-D) components of the E8870 chip set
- One P64H2 PCI-X bridge component (to drive SCSI controller and NIC)
- SCSI Ultra320 Controller
- Network Interface Controller (NIC) 10/100/1000 Ethernet controller that provides two LAN ports
- One I/O Control Hub 4 (ICH4) component
    — Four USB 1.1 ports (two at the rear, two through the front panel)
    — One IDE bus routed through the flex cable to the front panel board supporting one ATA33 master device
- Low Pin Count (LPC) Super I/O* with one external serial port and an internal header for a second port
- Integrated ATI* Rage* XL video controller and memory with two video ports – one at the rear and one through the front panel. The front panel video port supports resolutions up to 800x600.
- 8-MB Flash using four Firmware Hub (FWH) components
- Two VHDM connectors for PCI riser board
- One retention mechanism for processors and power pods
- In-Target Probe (ITP) port
- 200 MHz Front Side Bus (FSB)
- Four 400-MHz Rambus channels for memory interface
- Core ratio programming via the SNC-M
- Server management logic support
- Joint Test Action Group (JTAG) / boundary scan support through ITP or external source
- Clock buffering
- Six I^2C system management buses (SMBus)
- Embedded D2D converters
- BMC server management controller
- Power control - Advanced Configuration and Power Interface (ACPI)
- Speaker control
- I^2C logic
    — Includes Field Replaceable Unit (FRU) device ID that is accessed through a private I^2C bus
    — Temperature sensors
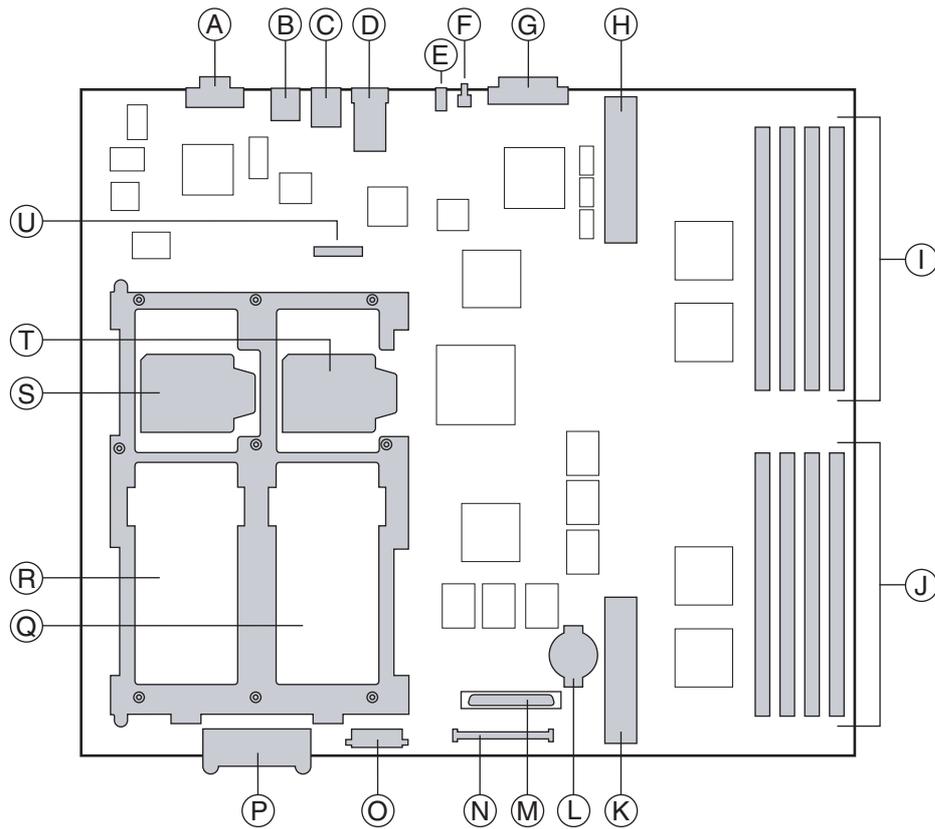
A. Video connector   B. COM2 connector
C. Dual USB connector   D. Dual gigabit Ethernet connector
E. System ID LED   F. System ID PB
G. External SCSI connector   H. VHDM 1
I. DIMM sockets 8, 4, 7, 3 from left to right   J. DIMM sockets 6, 2, 5, 1 from left to right
K. VHDM 0   L. Battery
M. Internal SCSI connector   N. 120-pin SM connector
O. PPOD connector   P. DC docking connector
Q. Processor power pod 2   R. Processor power pod 1
S. Processor 1   T. Processor 2
U. ITP connector   V.

Figure 17. Main Board Layout

Processor Sockets

Each Intel Itanium 2 processor plugs into a 700-pin Zero Insertion Force (ZIF) socket. Each processor is powered by a 12 V power pod located adjacent to the processor on the main board. Attached to the top of each processor is a heat sink that dissipates thermal energy.

Memory Subsystem

The basic architecture of the memory subsystem is as follows:

- The DIMMs reside on the main board, between the PCI riser assembly and the chassis.
- Four Rambus channels run from the Scalable Node Controller (SNC) to each of the four Memory Repeater Hubs (MRH-D).
- There is one MRH-D device per Rambus channel.
- A single DDR branch channel is implemented off each MRH-D.
- Each DDR branch channel supports two 184 pin DDR DIMMs.
- The server system includes eight DIMM connectors in two rows.
- Each row of DIMM sockets supports four DDR DIMMs, one channel of each MRH-D, which collectively make-up a cache line.

The DIMM socket locations are shown in the figure below.
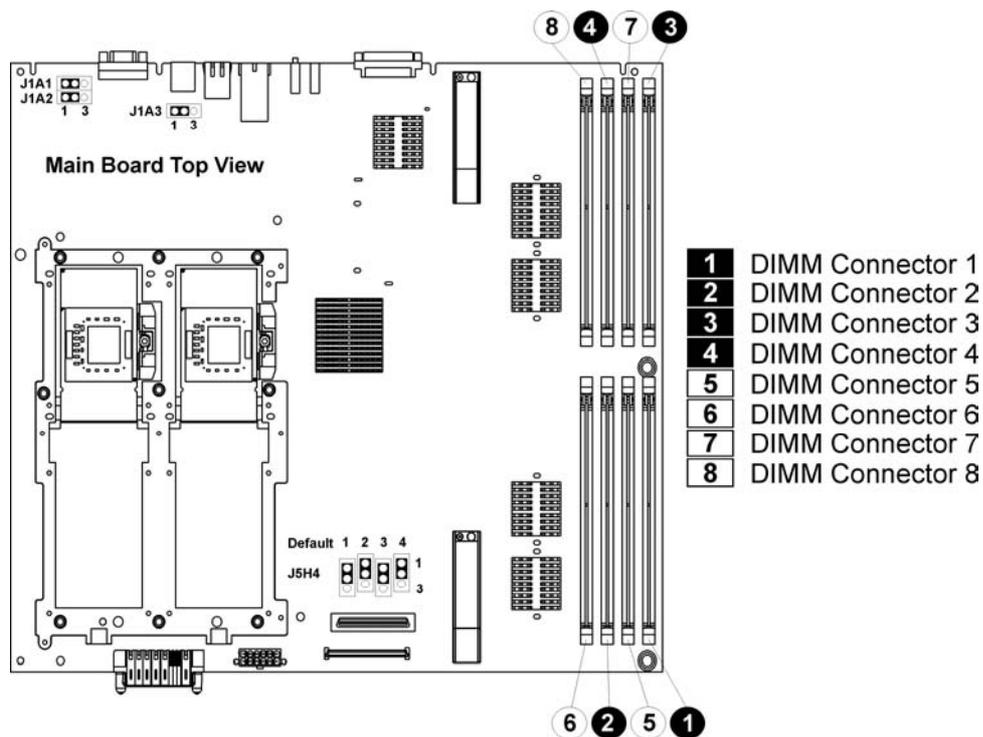
Figure 18. Location of Memory DIMMS

> The BIOS automatically detects, sizes, and initializes the memory array, depending on the type, size, and speed of the installed DIMMs. The BIOS reports memory size and allocation to the system through configuration registers.
>
> The system does not support mixed-sized DIMMs or DIMMs from different vendors within the same row.

DIMMs must be populated in groups of four, referred to as a row. Row 1 consists of DIMM sockets 1-4 and row 2 consists of DIMM sockets 5-8. The DIMM sockets in each row are not side-by-side; see *Figure 18* to identify each socket and row.

Within a single row, all DIMMs must be identical, both in DIMM size and the number of devices on the DIMM. Each of the two DIMM rows can be populated with DIMMs that use different technologies, but for the best performance, the amount of memory on each MRH-D DDR branch channel should be the same to enable the benefits of memory interleaving.

SCSI Controller

The LSI-531030 SCSI controller (U320) on the main board provides one primary channel to internal SCSI backplane and a secondary channel via an external SCSI connector at the rear of the chassis. This device interfaces to the SIOH at clock frequencies up to133MHz through one channel of the primary P64H2, also located on the main board. The 53C1030 is a fully autonomous device, capable of managing multiple I/O operations and associated data transfers from start to finish without host intervention.

While the internal channel supports only Low Voltage Differential (LVD) signaling, the external channel supports both LVD and SE (single-ended) signaling. With LVD signaling, the channels can each support a maximum data rate of 320 MB/sec.

Network Interface Controller

The onboard network interface is comprised of one Intel 82546EB Dual Port Gigabit Ethernet controller connected to the second channel of the primary P64H2 PCI-X bridge, located on the main board, at clock frequencies up to133MHz. The 82546EB is a single component with two fully IEEE 802.3 compliant Ethernet interfaces. It provides two stacked RJ45 ports at the rear of the chassis.

This network interface supports Ethernet applications at 1000Base-T, 100Base-T, and 10Base-T (802.3, 802.3u and 802.3ab) and enables network manageability implementations required for remote control and alert over LAN.

Video Controller

The onboard, integrated ATI RAGE XL 64-bit SVGA chip contains an SVGA controller that is fully compatible with industry video standards. The video sub-system implements 8 MB of 10-nanosecond onboard video memory.

The video controller supports pixel resolutions of up to 1600 x 1200 and up to 16.7 million colors and provides hardware-accelerated bit block transfers of data. The SVGA controller supports analog VGA monitors (single and multiple frequency, interlaced and noninterlaced) with a maximum vertical retrace noninterlaced frequency of 100 Hz.

Video connectors are located at both the front and the rear of the chassis. The connectors are auto sensed and only one can be used at a time. The connector at the front of the chassis supports resolutions up to 800x600.

IDE Controller

The IDE controller is contained within the Intel® ICH4 (82801DA). The IDE controller is a multifunction device on the I/O board that acts as a PCI-based Fast IDE controller. Although the server system implements a single IDE channel on the front panel board, which supports a CD/DVD drive at ATA-33 speeds, the IDE controller supports the following:

- PIO and IDE DMA/bus master operations
- Mode 4 timing
- ATA-100 (100MB/sec using ultra DMA transfers)
- Buffering for PCI/IDE burst transfers
- Master/slave IDE mode

Baseboard Management Controller (BMC)

The Baseboard Management Controller and its associated circuitry reside on the main board. The BMC autonomously monitors system platform management events and logs their occurrences in the non-volatile System Event Log (SEL). This includes events such as over-temperature and over-voltage conditions, and fan failures. The BMC provides the interface to the monitored information so system management software can pole and retrieve the present status of the platform.

The BMC provides the interface to the non-volatile Sensor Data Record (SDR) Repository. 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 (such as temperature and voltage sensors) in the system.

The following is a list of the major functions of the BMC:

- System power control, including providing Sleep/Wake push-button interfaces for ACPI
- Platform Event Paging / Platform Event Filtering
- Power distribution board monitoring
- Temperature and voltage monitoring
- Fan failure monitoring
- Processor presence monitoring (no processors installed)
- Interlock monitoring
- Speaker beep capability on standby and when system is powered up
- Intel Itanium 2 processor SEEPROM interface (for processor information ROM and scratch EEPROM access)
- Processor temperature monitoring
- Processor core ratio speed setting
- Chassis general fault light control
- Chassis cooling failure light control
- Chassis power fault light control
- Chassis power light control
- Chassis ID LEDs control
- System Event Log interface
- Sensor Data Record repository interface
- SDR/SEL timestamp clock
- Board set FRU information interface
- Fault resilient booting
- System management watchdog timer
- Front panel system diagnostic-interrupt handling
- Platform Management Interruption / System Diagnostic Interrupt status monitor
- Event receiver
- System interface to the IPMB (via system interface ports)
- IPMI Management Controller Initialization Agent
- Emergency Management Port interface
- Serial/modem and LAN alerting

The firmware for the BMC is field-upgradeable using the Firmware Update utility..

PCI Riser Board

The PCI riser board connection layout is displayed in *Figure 19*. It supports the following features:

- One Server I/O Hub (SIOH) component of the E8870 chip set
- One P64H2 component
- Three non-hot-plug PCI slots
  — One 64-bit, 133 MHz PCI-X, full length
  — Two 64-bit, 100 MHz PCI-X, full-length
- One integrated D2D
- Server management logic
- I^2C logic
  — FRU device ID accessed through a private I^2C bus
  — Temperature sensor

TP00351
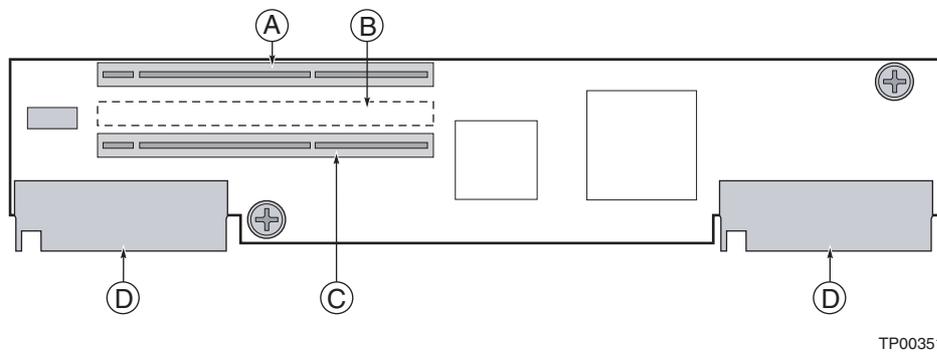
A. PCI slot 2
B. PCI slot 1 (on reverse side of board)
C. PCI slot 3
D. VDHM1 (left), VDHM0 (right)

Figure 19. PCI Riser Board Layout

SCSI Backplane Board

The SCSI backplane board connection layout is shown in *Figure 20*. The SCSI backplane board communicates with the main board via a 68-pin SCSI cable and to the Front Panel board via a 20-pin ribbon cable. It contains two industry standard 80-pin Single Connector Attachment (SCA)-2 connectors for hot-swap hard drives. Ultra320 or lower SCSI technology SCA type hard drives can be installed in this carrier. The backplane board accepts hard drives up to 15,000-RPM.

The features supported by the SCSI backplane board include the following:

- Monitoring the SCSI bus for enclosure services messages and acting on them appropriately. Examples of such messages include: activate a drive fault indicator, power down a drive that has failed, and report SCSI backplane temperature.
- SAF-TE intelligent agent, which acts as proxy for "dumb" I^2C devices during intra-chassis communications. "Dumb" I^2C devices are those that have no bus mastering capability.

The SCSI backplane provides three main functions for the system:

- It passes the SCSI signals between the main board and the SCSI drives
- It provides hooks for enclosure management
- It provides an I^2C server management interface

The SCSI backplane functional blocks include the following:

- Ultra320 LVD SCSI bus passes SCSI signals between the SCSI drives and the main board
    — A standard 68-pin SCSI connector provides the SCSI connection from the main board to the SCSI backplane
    — Two 80-pin (SCA-2 blind-mate) connectors are located on the SCSI backplane board to mate with hot-swap LVD SCSI drives in the drive bay
- Fault Tolerant Enclosure Management
    — SAF-TE
    — SCSI power control
    — LED control logic
- Server management
    — I^2C interface
    — I^2C Serial CMOS EEPROM (FRU)
    — Temperature sensor
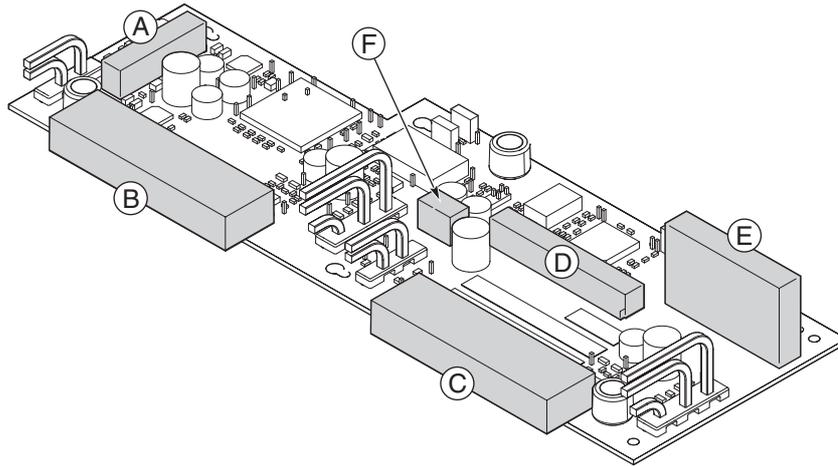
TP00354

Power bay connector

A. SCSI drive 1 connector   B. SCSI drive 2 connector
C. SCSI connector to main board   D. Front panel ribbon cable connector
E. Front panel power connector   F.

Figure 20. SCSI Backplane Board Layout

QLogic* GEM359* SCSI Hot-swap Controller

The QLogic GEM359 Hot-swap Controller resides on the SCSI backplane board. The primary functions of the GEM359 are as follows:

- Implements the SAF-TE command set
- Controls the SCSI hard drive fault LEDs
- Provides a path for management information via the SCSI
- Retrieves hard drive fault status, SCSI backplane temperature, and fan failure information via the IPMB
- Queries the status of the power distribution board by retrieving information from the BMC via the IPMB
- Controls hard drive power-on and power-down, facilitating hot-swapping

Front Panel Board

The front panel board connection layout is displayed in *Figure 21.* The front panel board provides three main functions for the system:

- It passes the IDE signals between the main board and the DVD drive
- It provides the front panel interface for the system
- It provides I^2C server management interface

Front Panel Board Functional Blocks

- IDE bus passes IDE signals between the IDE DVD and the main board
  — The 120 pin flex cable connector from main board provides IDE connectivity and auxiliary signals
  — Single IDE channel pass-thru connection to IDE connector for support of an IDE peripheral
- Front panel functions
  — Two USB 1.1 connections
  — Power, Reset, SDINT and ID buttons
  — LEDs for power, both NIC channels, ID, system and drive failure
  — VGA connector providing video from main board controller
- Server management
  — I^2C isolation to SCSI board
  — Temperature sensor
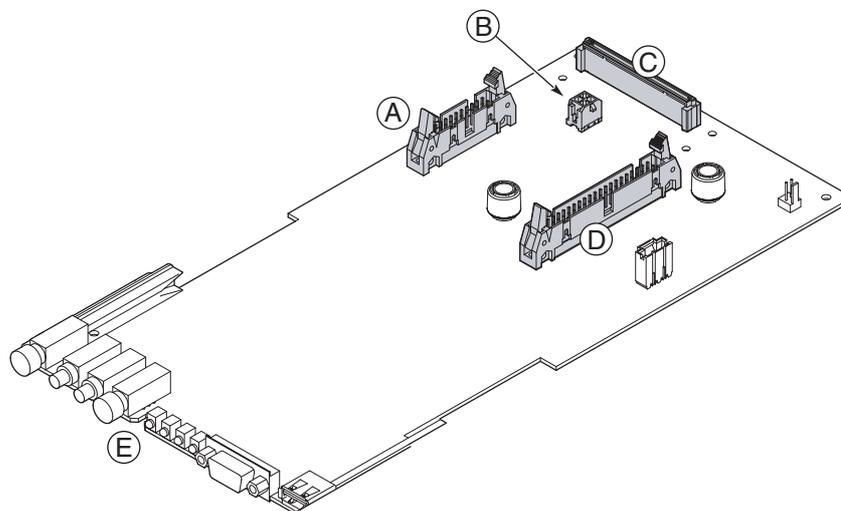
TP00355

A. Ribbon connector to SCSI backplane board
B. Power connector from SCSO backplane board
C. Flex cable to main board
D. IDE connector
E. Front panel buttons, LEDs, USB, video connector
F.

Figure 21. Front Panel Board Layout

3 Configuration Software and Utilities

Utilities / Drivers on Resource CD

The Resource CD included with your server system includes the following utilities and drivers that can be used to configure your system:

- LSI Logic SCSI Driver for Linux (64-bit) and Windows* 2003 Server
- Utilities:
  — FRUSDR Loader
  — EFI Platform Diagnostics
  — System Maintenance Utility (SMU)
    - SDRViewer
    - SELViewer
- EFI Configuration Tool

The Resource CD includes a menu driven program that can be used for the following:

- Create a diskette containing drivers for various operating systems.
- Install EFI Service Partition. The EFI service partition provides the ability to remotely access the server via modem or LAN for the purpose of executing configuration/setup utilities and diagnostics.
- Run EFI-based utilities.

Running Software Utilities Directly from the Resource CD

The following procedure allows you to run the software utilities directly from the Resource CD.

1. Insert the System Resource CD into the server's CD-ROM drive before booting to EFI Shell.
2. Boot the system into EFI Shell, the EFI CD menu program launches automatically. If the EFI CD menu program does not launch in the EFI Shell, mount and map to the CD drive and type `startup` and press `<Enter>` to launch the EFI CD menu.
3. Move the curser to the Utilities and select the utility you want to run.

Power-on Sequence and Power-on Self-Test (POST)

Turning on the system causes POST to run and control to pass to the boot manager. From the boot manager, you can choose to invoke the Extensible Firmware Interface (EFI) Shell or you can choose to go to the Boot Maintenance menu.

The system follows the steps below when you press the power button on the front control panel to power up the server:

1. The server fans start.
2. POST begins running. POST is stored in flash memory. It checks the drive carriers, processors, memory, keyboard, and most installed peripheral devices. During the memory test, POST displays the amount of memory it is able to access and test. The length of time needed to test the memory depends on the amount of memory installed.

3. Video appears on the monitor that is attached to the server and begins to display boot progress. The AMI* BIOS banner displays the loaded versions of the BIOS, PAL, SAL, and EFI.
4. POST concludes and passes control to the boot manager.
5. From the boot manager, you can use arrow keys to highlight the option that invokes the EFI shell operating system if it is installed, or you can highlight and select the Boot Maintenance menu. Selecting the Boot Maintenance menu lets you configure boot options and other boot environment variables. Booting to the EFI shell causes the following prompt to appear: `Shell>`
6. When you see this prompt, you can load and start an operating system.

Extensible Firmware Interface Boot Manager

The EFI boot manager allows you to control the server's booting environment. Depending on how you have configured the boot options, after the server is powered up the boot manager presents you with different ways to bring up the system. For example, you can boot to one of the following:

EFI Shell: An interactive environment that allows EFI device drivers to be loaded, EFI applications to be launched, and operating systems to be booted. The EFI shell provides a set of basic commands used to manage files and the system environment variables. For more information on the EFI Shell, see *The Extensible Firmware Interface (EFI) Shell*, on page 34.

Boot Options: Files that you include as boot options. You add and delete boot options by using the Boot Maintenance menu. Each boot option specifies an EFI executable with possible options. For information on the Boot Maintenance menu options, see *Table 4*.

Boot Maintenance Menu: A menu of items allowing you configure boot options and other boot environment variables. Table 4 describes each menu item in the Boot Maintenance menu.

Table 4.   Boot Maintenance Menu Options

Option	Description
Boot from a File	Automatically adds EFI applications as boot options or allows you to boot from a specific file.
	When you choose this option, the system searches for an EFI directory in all EFI System Partitions in the system. For each EFI directory that the system finds, it searches through that directory's subdirectories for the first file that is an executable EFI application. Each file that meets this criterion can be automatically added as a boot option. In addition, legacy boot options for A: and C: are also added if those devices are present.
	With this option, you can launch a specific application without adding it as a boot option. In this case, the EFI Boot Manager searches the root directories of all of the EFI System Partitions present in the system for the specified EFI application.
	To boot from a file:
	• At the menu, use the arrow key to select `Boot from a File`.
	• Press `<Enter>` to select the option.
	• Use the arrow key to choose the EFI file to boot from.
	• Press `<Enter>` to select the option.

Option	Description
Add a Boot Option	Adds a boot option to the EFI Boot Manager. You specify the option by providing the name of the EFI application. You can provide either ASCII or UNICODE arguments that the file might use.
	Given the EFI application name and any options, the EFI Boot Manager searches for the executable file in the same partitions and directories as described in `Boot from a File`. When the file is found, it is executed.
	To add a boot option:
	• At the menu, use the arrow key to select `Add Boot`.
	• Press `<Enter>` to select the option.
	• Type in the name of the EFI application and press `<Enter>`.
	• Select `Save to NVRAM`.
	• Select `Exit` to return to the Boot Manager.
Delete Boot Options	This feature allows you to delete a specific boot option or all boot options. To delete boot options:
	• At the menu, use the arrow key to select `Delete Boot Option`.
	• Press `<Enter>` to select the option.
	• Use the arrow keys to select the boot option to delete.
	• Press `<Enter>` to select the option.
	• Press `<Y>` to confirm your selection.
	• Select `Save to NVRAM`.
	• Select `Exit` to return to the Boot Manager.
Change Boot Order	This feature allows you to control the relative order in which the EFI Boot Manager attempts boot options. For help on the control key sequences you need for this option, refer to the help menu. To change the boot order:
	• At the menu, use the arrow key to select `Change Boot Order`.
	• Use the arrow keys to select the Option to `move`.
	• Press `<u>` to move up in the boot order.
	• Press `<d>` to move down in the boot order.
	• Select `Save to NVRAM`.
	• Select `Exit` to return to the Boot Manager.
Manage BootNext Setting	This feature allows you to select a boot option to use one time (the next boot operation).
	To manage boot next setting:
	• At the menu, select `Manage Boot Next Setting` with the arrow key.
	• Select the Option to `boot next` with the arrow key.
	• Press `<b>` to make this option the next boot option.
	• Press `<r>` to reset.
	• Select `Save to NVRAM`.
	• Select `Exit` to return to the Boot Manager.

Option	Description
Set Auto Boot Timeout	This feature allows you to define the value in seconds that pass before the system automatically boots without user intervention. Setting this value to zero disables the timeout feature.
	To set auto boot timeout:
	- At the menu, select `Set Auto Boot Timeout` with the arrow key. - Three options are available. - Select the `Choose Value` option with the arrow key and enter a value of "0" to disable auto boot. - Select the `Delete` option with the arrow key and select the Delete setting with the arrow key and press `<Enter>`. - Choose a time out value of 65535 (0xFFFF) to allow you to press any key while booting to EFI to disable timeout.
Select Console Output Device	This feature allows you to select the device that the console output is sent to.
	To select the console output device:
	- At the menu, select `Manage Boot Next Setting` with the arrow key. - Select the Option to `boot next` with the arrow key - Press `<b>` to make this option the next boot option. - Press `<r>` to reset. - Select `Save to NVRAM`. - Select `Exit` to return to the Boot Manager.
Select Console Input Device	This feature allows you to select the device that the console receives input from.
	To select the console input device:
	- At the menu, select `Manage Boot Next Setting` with the arrow key. - Select the Option to `boot next` with the arrow key. - Press `<b>` to make this option the next boot option. - Press `<r>` to reset. - Select `Save to NVRAM`. - Select `Exit` to return to the Boot Manager.
Select Standard Error Device	This feature allows you to select the standard error device.
	To select the standard error device:
	- At the menu, select `Manage Boot Next Setting` with the arrow key. - Select the Option to `boot next` with the arrow key. - Press `<b>` to make this option the next boot option. - Press `<r>` to reset. - Select `Save to NVRAM`. - Select `Exit` to return to the Boot Manager.
Cold Reset	Performs a platform-specific cold reset of the system. A cold reset means a full platform reset.
	To perform a cold reset:
	- At the menu, select `Set Auto Boot Timeout` with the arrow key. - Press `<Enter>`. - The system resets.

Option	Description
Exit	Returns control to the EFI Boot Manager main menu. Selecting this option displays the active boot devices, including a possible integrated shell.

The Extensible Firmware Interface (EFI) Shell

The EFI shell application allows other EFI applications to be launched, EFI device drivers to be loaded, and operating systems to be booted. The combination of the EFI firmware and the EFI shell provides an environment that can be modified to easily adapt to many different hardware configurations.

The EFI shell provides a set of basic commands used to manage files and EFI NVRAM shell and boot variables. A list of these basic commands is shown in Table 5. Descriptions of the EFI shell commands are also available when operating in the EFI Shell. To access the descriptions, type `help` and press the `<Enter>` key.

Table 5.   EFI Shell Commands

Command	Description
`<drive_name>:`	Changes drives. For example, entering fs0: and pressing the `<Enter>` key changes the drive
`alias [-bdv] [`*sname*`] [`*value*`]`	Sets or gets alias settings
`attrib [-b] [+/- rhs] [`*file*`]`	Views or sets file attributes
`bcfg -?`	Configures boot driver and load options in EFI NVRAM
`botmaint`	Launches Boot Maintenance Manager
`break`	Executes a breakpoint
`cd [`*path*`]`	Changes the current directory
`cls [`*background color*`]`	Clears the screen
`comp `*file1 file2*	Compares two files
`connect [-r] [-c] Handle#` `½DeviceHandle# DriverHandle#`	Binds the EFI driver to a device and starts the driver
`cp [-r] `*file*` [`*file*`] ... [`*dest*`]`	Copies files and directories, [-r] = recursive
`date [`*mm*`/`*dd*`/`*yyyy*`]`	Gets or sets the date
`dblk device [Lba] [Blocks]`	Performs a hex dump of BlkIo Devices
`devices [-b] [-1XXX]`	Displays devices
`devtree [-b] [-d]`	Displays device tree
`dh [-b] [-p `*prot_id*`]	[`*handle*`]`	Dumps handle information
`disconnect DeviceHandle#` `[DriverHandle# [ChildHandle#]`	Disconnects device from driver
`dmem {address] [size] [;MMIO]`	Displays the contents of memory
`dmpstore`	Dumps the variable store
`drivers [-b] [-lXXX]`	Displays drivers
`drvcfg [-c] [-lXXX] [-f] [-v] [-s]`	Invokes the driver configuration protocol
`drvdiag [-c] [-lXXX] [-s] [-e] [-m]`	Invokes the driver diagnostics protocol
`echo [[-on	-off]	[text]`	Echoes text to the standard output device or toggles script echo
`edit [`*filename*`]`	Opens the text editor allowing you to create or edit a file
`eficompress infile outfile`	Compresses an EFI file
`Efidecompress infile outfile`	Decompresses an EFI file
`endfor`	Provides a delimiter for loop constructs (scripts only)
`endif`	Provides a delimiter for IF THEN constructs (scripts only)

Command	Description
`for var in <set>`	
`goto label`	Makes batch file execution jump to another label
`guid [-b] [sname]`	Dumps known guid ids
`help [-b] [internal_command]`	Displays help information
`hexedit [[-f]FileName|[-d DiskName Offset Size]|[-m Offset Size]]`	Edits in HEX mode
`if [not] condition then`	Provides conditional constructs (scripts only)
`load driver_name`	Loads a driver
`loadbmp [-c] [-t] [-i[UGA Instance]] file`	Displays a bitmap file on the screen
`loadpcirom romfile`	Loads a PCI option ROM
`ls [-b] [dir] [dir] ...`	Obtains directory listings
`map [-bdvr] [sname[:]] [handle]`	Maps *sname* to device path
`mem [address] [size] [;MMIO]`	Dumps Memory or Memory Mapped IO
`memmap [-b]`	Dumps memory map
`mkdir dir [dir]`	Creates a new directory
`mm address [Width] [;Type] [n]`	Memory Modify: type = Mem, MMIO, IO, PCI, [n] for non interactive mode when inside a .nsh file
`mode [col row]`	Sets or gets the current graphics mode
`mount BlkDevice [sname[:]]`	Mounts a file system on a block device
`mv [src…] [dst]`	Move one or more files/directories to destination
`pause`	Prompts to quit or continue (scripts only)
`pci [bus_dev] [func]`	Displays PCI device information
`rconnect DeviceHandle# [DriverHandle# [ChildHandle#]]	[-r]`	Reconnects one or more drivers from a device
`reset [reset_string]`	Performs a cold reset
`rm file/dir [file/dir]`	Removes files or directories
`setsize file`	Sets size of a new file
`stall microseconds`	Delays for the specified number of microseconds
`time [hh:mm:ss]`	Gets or sets the time
`type [-a] [-u] [-b] file`	Displays the contents of a file
`ver`	Displays version information
`vol fs [volume_label]`	Sets or displays a volume label

BIOS Setup

This section describes the BIOS Setup Utility, which is used to change the server configuration defaults. You can run the utility with or without an operating system present on the server. Setup stores most of the configuration values in battery-backed CMOS and the rest in flash memory. The values take effect when you boot the server. POST uses these values to configure the hardware. If selected values and the hardware do not agree, POST generates an error message and you must then run Setup to specify the correct configuration.

Run Setup to view or modify such server board features as:

- Serial port configuration
- Time/date (to be stored in RTC)
- IDE settings (DVD/CD-ROM, etc.)
- SCSI BIOS
- Default CMOS settings and fail safe settings
- Password security
- Advanced chip set settings for boot up
- Information on system configuration, version, peripheral population, RAM size, and cache size

Starting Setup

To start Setup during the power-on sequence, follow these steps:

1. Press the power button on the front control panel of the server. .
2. When POST shows the message "`Press <F2> if you want to run SETUP`," press <F2>. If the server has an administrator password configured, the system prompts you to enter the password. If the server does not have a password configured, the main screen of the BIOS Setup Utility appears.

Recording Your Setup Settings

Before you make any changes, record the current values. If the default values need to be restored later, such as after a CMOS clear, you must run Setup again. Referring to recorded original settings could make your task easier.

Navigating Setup Utility Screens

The BIOS setup utility consists of five primary menus:

Main: Displays the BIOS version and details on processor type, and lets you configure the system time, date, and language.

Advanced: Lets you configure Option ROMs, configure peripheral devices, clear the event log, and disable POST error pauses.

Security: Lets you set a password.

System Management: Lets you configure Console Redirection, Quite Boot, Serial Over LAN, and Service Partition options. Also displays BMC and HSC firmware revisions.

Exit: Exits the utility with or without saving utilities and allows management of custom settings.

Each menu occupies a single screen and presents a list of menu items. Some menu items are sub-menus, while others are settings that you can change from the screen.

Table 6 describes how to navigate between the utility screens and menus.

Table 6.   Setup Screen Navigation

Press	To
←	Scroll left through the main menu screens.
→	Scroll right through the main menu screens.
ENTER	Select a sub-menu item or accept a drop-down choice.
TAB	Select a field within a value (for example, date field).
F9	Select the default value.
F10	Save your changes and exit Setup.
ESC	Go back to a previous screen.
↑	Scroll up through menu items or value lists.
↓	Scroll down through menu items or value lists.

Setup Screens

Main

Table 7 describes the menu items available on the Main screen. Default values appear in brackets. *Table 8* provides the settings for the processor. This submenu is available from the Processor Settings option on the Main menu.

Table 7.   BIOS Setup Main Screen Menu Items

Menu Item	Default Value	Description
System Time	HH:MM:SS	Set the System Time in *hour:minute:second* format.
System Date	MM/DD/YYYY	Set the System Date in *month/day/year* format.
Processor Configuration	Press <Enter> to present selection submenu	Selects the sub-menu. See *Table 8*.
Language	[English (US)] Spanish Italian French German	Selects the language that the BIOS displays.
BIOS Version	[*bios_version_number*]	The currently loaded version of BIOS. You cannot change this value. It appears for informational purposes only.
PAL Version	[PAL_*version_number*]	The currently loaded version of PAL. You cannot change this value. It appears for informational purposes only.
SAL Version	[SAL_*version_number*]	The currently loaded version of SAL. You cannot change this value. It appears for informational purposes only.
FPSWA Version	[FPSWA_*version_num*]	The currently loaded version of FPSWA. You cannot change this value. It appears for informational purposes only.

Table 8.   Processor Settings Submenu Items

Menu Item	Default Value	Description
Processor Retest	[No] Yes	If yes, BIOS clears historical processor status and retests all processors on the next boot.
Processor POST speed setting	Information Only	Displays measured processor speed. Shows common operating processor speed.
Processor 1 CPUID	N/A	Reports CPUID for Processor 1.
Processor 1 L1 Cache Size	N/A	Reports L1 Cache Size for Processor 1.
Processor 1 L2 Cache Size	N/A	Reports L2 Cache Size for Processor 1.
Processor 1 L3 Cache Size	N/A	Reports L3 Cache Size for Processor 1.
Processor 2 CPUID	N/A	Reports CPUID of the Processor 2.
Processor 2 L1 Cache Size	N/A	Reports L1 Cache Size for Processor 2.
Processor 2 L2 Cache Size	N/A	Reports L2 Cache Size for Processor 2.
Processor 2 L3 Cache Size	N/A	Reports L3 Cache Size for Processor 2.

Advanced

Table 9 describes the menu items available on the Advanced screen. Five menu items exist on this screen. Each of these items contains sub-menus that in turn can also lead to subsequent sub-menus. Default values appear in brackets.

Table 9.   BIOS Setup Advanced Screen Menu Items

Primary Menu Item	Sub Menu Items	Value	Description
Peripheral Configuration	Serial Port	[Auto] Enabled Disabled	Determines Serial Port configuration at boot time. Auto Causes the server to determine the Base I/O address and interrupt to use for the port. Enabled Requires you to supply the Base I/O address and the interrupt value. Disabled Causes the server to disable the port.
Option ROM Configuration	PCI SLOT 1 ROM	[Enabled] Disabled	Enables Slot 1 Option ROM.
	PCI SLOT 2 ROM	[Enabled] Disabled	Enables Slot 2 Option ROM.
	PCI SLOT 3 ROM	[Enabled] Disabled	Enables Slot 3 Option ROM.
Event Log Configuration	SEL Event Logging	[Enabled] Disabled	Enabled allows logging of system events.
	Clear All Event Logs	[No] Yes	Instructs the BMC to clear the SEL log.
POST Error Pause		[Enabled] Disabled	Select `Disabled` if you want the system to boot with no user intervention on critical POST errors.

Security

Table 10 describes the menu items available on the Security screen.

📝 **NOTE**

> With the removal of legacy keyboard and mouse support, the legacy security core has been removed. Therefore, the security menu is brief as compared to other server products. The two-level password has been replaced with a single-level password.

Table 10.   BIOS Setup Security Screen Menu Items

Menu Item	Default Value	Description
Administrator Password Is	[Not Installed] Clear	Status only. Once set, can be disabled by setting to a null string, or clear password jumper on the main board.
Set Admin Password	Press <Enter>	When the <Enter> key is pressed, you are prompted for a password, press ESC key to abort. Once set, can be disabled by setting to a null string, or clear password jumper on the main board.

System Management

Table 11 describes the menu items available on the System Management screen. Default values appear in brackets.

Table 11.   BIOS Setup System Management Screen Menu Items

Menu Item	Default Value	Description
Quiet Boot	[Disabled] Enabled	Selecting this option enables the BIOS to display the OEM logo during POST. If disabled, the BIOS displays the normal POST messages. This option is shaded if the BIOS does not detect a valid logo in the flash area reserved for this purpose. Enabling this option disables serial redirection.
OS Boot Timeout	[Disabled] 5 min 10 min 15 min 20 min	Sets the time allowed for booting an operating system, from media or PXE.
Service Boot	[Disabled] Enabled	Enabling this item allows you to boot into Service Partition Boot mode. The item automatically resets to Disabled on the next system boot.
Console Redirection	Press `<Enter>` to present selection submenu	Selecting this option allows you to configure for console redirection.
BMC Revision	*[BMC_Rev]*	The currently loaded version of Baseboard Management Controller firmware. Display only.
HSC Revision	No entry	Displays the revision of the hot swap controller. Display only.

Table 12.   Setup Console Redirection Sub Menu Items

Sub Menu Item	Default Value	Description
Serial Console Redirection	[Disabled] Enabled	When enabled, Console Redirection uses only COM2. Choosing "Disabled" completely disables Console Redirection.
Serial Port	No entry	Hardcoded value is COM2 2F8 IRQ3. If console redirection is enabled, then the Base I/O address and IRQ selection of Serial Port B should match this serial port setting under the Console Redirection submenu. To find this option, go to the Advanced menu, then Peripheral Configuration.
Baud Rate	9600 [19.2K] 38,4K 57.6K 115.2K	When Console Redirection is enabled, use the baud rate specified. When the EMP is sharing the COM port as console redirection, the baud rate must be set to 19.2K to match the EMP baud rate.
Flow Control	No Flow Control [CTS/RTS] XON/XOFF CTS/RTS + CD	No flow control. CTS/RTS = Hardware based flow control. CTS/RTS +CD = Hardware based + Carrier Detect flow control. When the EMP is sharing the COM port as console redirection, the flow control must be set to CTS/RTS or CTS/RTS+CD depending on whether a modem is used.
Terminal Type	[PC-ANSI] VT100+	Select terminal type. Vt100+ only available when English selected as the language. VT-UTF8 uses UNICODE. PC-

Sub Menu Item	Default Value	Description
	VT-UTF8	ANSI is the standard PC-type terminal
Remote Console Reset	[Disabled] Enabled	Enables remote reset via escape key sequence; ESC R ESC r ESC R
ACPI OS Headless Operation	Disabled Same as BIOS Serial Port	Passes information about serial redirection to ACPI OS.
ACIP OS Baud Rate	9600 [19.2K] 38.4K 57.6K 115.2K	Available only when ACPI OS Headless Operation is the same as BIOS or serial port.
ACPI OS Flow Control	No Flow Control [CTS/RTS] XON/XOFF CTS/RTS + CD	Available only when ACPI OS Headless Operation is the same as BIOS or serial port. Options are passed to the operating system.
ACPI OS Terminal Type	PC-ANSI VT100+ VT-UTF8	Available only when ACPI OS Headless Operation is the same as BIOS or serial port. Options are passed to the operating system.

Exit

Table 13 describes the menu items available on the Exit screen. Default values appear in brackets.

Table 13.   BIOS Setup Exit Screen Menu Items

Menu Item	Description
Exit Saving Changes	Lets you exit Setup with or without saving your changes in CMOS. Clicking on the menu item causes the system to prompt you for a Yes or No response. Yes Saves your changes and exits the utility. No Discards your changes and exits the utility.
Exit Discarding Changes	Lets you exit Setup with or without discarding your changes. Clicking on the menu item causes the system to prompt you for a Yes or No response. Yes Discards your changes and exits the utility. No Saves your changes and exits the utility.
Load Setup Defaults	Lets you load Setup with factory defaults. Clicking on the menu item causes the system to prompt you for a Yes or No response. Yes Loads the system setup defaults. No Aborts the action.
Load Custom Defaults (This menu is not available until POST platform release)	Lets you load Setup with custom defaults. Clicking on the menu item causes the system to prompt you for a Yes or No response. Yes Loads setup values from a file previously saved through the Save Custom Defaults menu item. You must specify the file name. No Aborts the action.
Save Custom Defaults	Stores current CMOS settings in custom default CMOS area (flash).
Discard Changes	Lets you discard the changed values you have accumulated during this setup session. Clicking on the menu item causes the system to prompt you for a Yes or No response. Yes Discards the setup values for the current setup utility session. No Aborts the action.

LSI Logic* SCSI Utility

The LSI Logic* SCSI utility allows you to configure the SCSI capabilities of the server. It allows creating a Mirror on the internal disks.

Please contact your Bull representative for more information on obtaining this utility

Launching the LSI SCSI Utility

To launch the LSI SCSI utility from the Resource CD:

1. The utility will auto-run if the server is booted with the CD in the CD-ROM/DVD-ROM drive. Otherwise, choose `Startup.nsh` from the root of CD-ROM/DVD-ROM drive.
2. After the CD menu is launched, select `Utility` at the top of the Main menu screen.
3. Select `EFI config tool` from the drop-down selections
4. Select `PCI Device` from the top of the next screen that is displayed.

To launch the LSI SCSI utility from the command line:

1. From the EFI Shell, run `EFICnfg.efi` to enter the LSI Logic SCSI Utility.
2. At the Main menu, select `PCI Device` at the top of the screen.

Creating a RAID1 (Mirror) on the internal disks

Activation

To activate the mirroring function on the NovaScale internal disks, proceed as described hereunder.

⚠ **CAUTION**

> When activating the mirroring, data on both disks will be lost.

1. Insert the NovaScale 4020 Resource CD, then boot the system
2. After the CD menu is launched, select `Utility` at the top of the Main menu screen
3. Select `EFI config tool`, then select `PCI Device`
4. From the PCI device drop-down menu, use the arrow keys to move to the line
   `On Board: Function1 LSI Logic Ultra320 SCSI Controller`
   then press `Enter` to select this option
5. Press `Enter` at the Configure prompt
6. Use the arrow keys to highlight `53C1030 Bus 3 Dev1 Fnc1`,
   then press `Enter` to select this adapter
7. Use the arrow keys to highlight `RAID Properties`, then press `Enter`
8. Use the arrow keys to select `Disk 0`, press the `<+>` key; this will activate the Help sceen
9. Press the `<D>` key; this will turn the Disk 0 to RAID=YES
10. Use the arrow keys to select `Disk 1`, press the `<+>` key; this will turn the Disk 1 to RAID=YES
11. Press the Esc key, Use the arrow keys to select `Save Changes then exit this menu`, then press `Enter`
12. A screen appears, showing `Creating RAID`. This operation lasts around one minute.
13. When RAID creation is completed, exit the EFI config tool.

At this time the SCSI controller starts the synchronization process (copy of the master disk contents on to the secundary disk). The LED of both disks blinks in green.

This operation is very slow when performed under EFI: around 1 hour per GB disk space.

If the system is powered down during the synchronization, when the system is powered on the synchronization restarts at the point it was interrupted.

Installation of the Operating System

The installation of an operating system on the disk may be conducted in parallel with the synchronization of the disks.

Proceed as usual for the installation of a Windows or Linux operating system.

The installation of an operating system, and later its use, greatly increases the speed of the synchronization process. When performed under OS running, the synchronization of 1 GB disk space lasts around 8 minutes.

With the Linux operating system, after having installed it, it is necessary to install the `IMUtility`.

This utility will allow correct operation of the HDDs LEDs and the hard drive fault LED on the front panel (see Behavior hereafter).

This utility is available on the NovaScale 4020 Resource CD or at the Bull supports Web site.

After having installed the utility, it is necessary to reboot the system to make it operational.

Behavior

The LEDs on both disks and the hard drive fault LED on the front panel allow to ascertain the current status of the RAID on the internal disks:

- In Normal operation (RAID function operational):
  — both LEDs on the 2 HDD drives blink simultaneously in green when I/O operations are performed
  — Hard drive fault LED on the front panel is off

- When one disk is in failure:
  — The LED on the HDD drive in failure blinks in Amber;
    the LED on the active HDD drive blinks in green when I/O operations are performed
  — The hard drive fault LED on the front panel is on (amber)
  — It is necessary to replace the disk in failure

- When one disk is missing:
  — The LED on the remaining HDD drive blinks in green when I/O operations are performed
  — The hard drive fault LED on the front panel is off

  If a new disk in inserted, the synchronization process immediately starts (see hereunder).

- When a disk synchronization process is active:

⚠ **CAUTION**

When operating in degraded mode (only one disk active), the synchronization process starts as soon as an operational disk is inserted in lieu of the disk in failure.

There is no message asking for the confirmation of the operation. The data on the newly inserted disk will be lost.

All along the synchronization the LEDs behave as follows:

— The LED on the HDD drive being synchronized blinks in Amber; the LED on the active HDD drive blinks in green

— The hard drive fault LED on the front panel blinks in amber

As soon as the synchronization process is completed the disks enter normal operation (see above).

System Maintenance Utility

The System Maintenance Utility is an EFI-based program that provides the ability to view or modify the server management firmware configuration, which is maintained by the BMC. The executable program for the SMU is smu.efi.

The SMU lets you:

- Configure serial/modem channels for remote server management over a modem or direct serial connection.
- Configure LAN channels for remote server management over the network.
- Configure users and associated passwords for channel access. Users and channels can be assigned privilege levels to further define the access levels.
- Configure platform events to define the actions that should take place when specific events occur.
- Configure serial over LAN and terminal mode capabilities.
- Configure the power restore policy for the server.
- View, save and clear the BMC System Event Log.
- View and save the BMC Sensor Data Records.
- View and save the Field Replaceable Unit records.

The SMU core components are installed as part of the service partition software installation process and the remote SMU application is part of the Intel® Server Management installation. SMU files are copied to a directory specified during that installation process. It is also possible to run the local SMU application from a CD without installing a service partition.

The SMU software consists of a user interface and core components. The user interface components present the user interface, gather user input, and send input to the core components. The core components interpret data and perform necessary actions to the hardware. The core components also maintain the state of the application and determine the screens to be shown. Specific state information is stored in the data that is exchanged between the user interface and core components.

The core components of the SMU are the same for the local and remote applications. If the SMU is run locally, the user interface and core components coexist on the same system and communicate using a procedural call interface. When run remotely, the user interface components and core components communicate use a socket interface. Running the remote SMU requires the use of Intel Server Management.

NOTE

The local SMU application is available only in English.

Remote Keyboard Navigation

The remote SMU application requires a pointing device for operation; it does not support accelerator keys. Other keys work as described in Table 14.

Table 14.   Keyboard Support for Remote SMU Client

Key	Function
`<Enter>`	Pressing `<Enter>` when focus is on a button causes the action associated with that button to occur.
`<Tab>`	Moves focus to the next control in the tab order in the primary information pane.
`<Shift><Tab>`	Moves focus to the previous control in the tab order.

Local Keyboard Navigation

The local SMU application provides keyboard support as follows:

Table 15.   Keyboard Support for Local SMU Client

Key	Function
`<Enter>`	If the cursor is in an edit box, the `<Enter>` key moves the cursor to the next selectable control in the currently active pane. When the focus is on a task menu item, a task button, a radio button, or a check box, pressing `<Enter>` selects the control. If the focus is on a single-select control (combo box), pressing `<Enter>` has no effect.
`<Tab>`	Moves focus to the next control in the tab order in the primary information pane.
`<Up arrow>`	Moves the cursor to the previous selectable control in the currently active pane.
`<Down arrow>`	Moves the cursor to the next selectable control in the currently active pane. (Same as the `<Tab>` key.)
`<Right arrow>`	Moves the cursor to the next selectable control in the currently active pane. (Same as the `<Tab>` key.)
`<Left arrow>`	Moves the cursor to the previous selectable control in the currently active pane. (Same as the `<UP arrow>` key.)
`<F5> key`	If a horizontal scroll bar is in the active pane, pressing `<F5>` scrolls the display left.
`<F6> key`	If a horizontal scroll bar is in the active pane, pressing `<F6>` scrolls the display right.
`<F7> key`	If a vertical scroll bar is in the active pane, pressing `<F7>` scrolls the display up.
`<F8> key`	If a vertical scroll bar is in the active pane, pressing `<F8>` scrolls the display down.
`<F10> key`	Toggles the focus between the task pane and the primary information pane.
`<ESC> key`	Displays the Exit dialog.

The following are true when using the above keys while running the local SMU application:

1. For single-select controls (combo boxes), the `<up arrow>` and `<down arrow>` keys can be used to move through the items in the list. To move to a different control, the `<Tab>`, `<left arrow>`, or `<right arrow>` keys are used.
2. For a set of grouped radio buttons from which only one can be selected, the `<up arrow>`, `<down arrow>`, `<left arrow>`, and `<right arrow>` keys can be used to move between buttons in the group. To move to a different control, the `<Tab>` key is used.
3. For edit box controls, the `<left arrow>` and `<right arrow>` keys can be used to move the cursor within the edit box. To move to a different control, the `<Tab>`, `<Enter>`, `<up arrow>`, or `<down arrow>` key are used.

About Box Information

The SMU includes an "About" item in the task pane when the task list is displayed. When `About` is selected, a dialog box is displayed showing information about the SMU application version. The information displayed consists of a set of four numbers, defined as follows:

- The major feature release number
- The minor platform or maintenance release number
- The variant, used for things like different operating systems or languages
- The build number

See the example below.
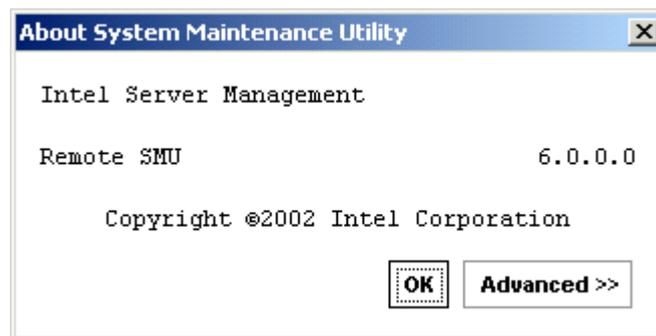
Figure 22. SMU Application About Box

The About box contains an `Advanced` button that can be used to show version information for components related to the SMU application. See the example below.
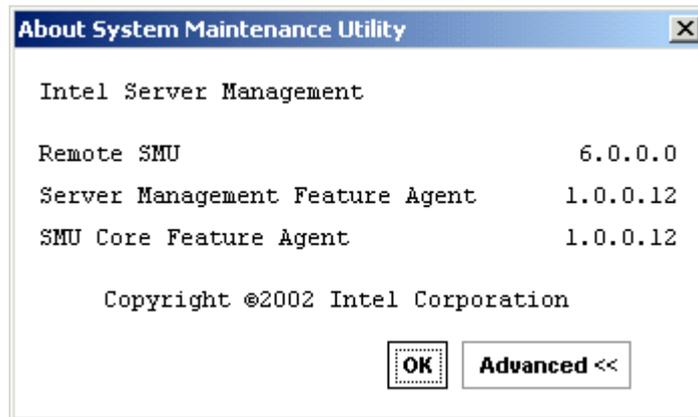
Figure 23. SMU Application About Box (Advanced button selected)

Server Discovery

The remote SMU application requires that the Intel Server Management software be installed on the client system. When the ISM software is run, it performs a discovery of all servers that support tools available within ISM. The discovered servers are displayed in the ISM Console. By clicking on a server name in the table, a list of tools supported on that server is displayed. The SMU is contained in the set of tools listed under the heading "Reboot to Service Partition".

Remote SMU Application

The path used to connect to a target server is defined by the ISM software, based on information it has about each server. After a LAN connection is established between the remote SMU application and SMU core components on the server, the application and the core components set up a socket connection to communicate through.

The sequence of steps that occur when starting the remote SMU application is listed below. These steps occur under the control of the ISM software, not the SMU software, and all errors are handled by the ISM software.

1. In the ISM Console software, click on `Reboot to Service Partition` under the list of tools for a server shown.
2. Enter the username and password for an out-of-band connection on the Service Partition Utilities screen.
3. Click `Login.`

4. When the server has been successfully rebooted to the service partition software, the supported service partition utilities are displayed, as shown below. Click on `System Maintenance Utility` to launch the SMU application. ISM passes connection information to the SMU so the SMU can communicate with the target server. Up to this point, all errors are handled by the ISM software, not the SMU.
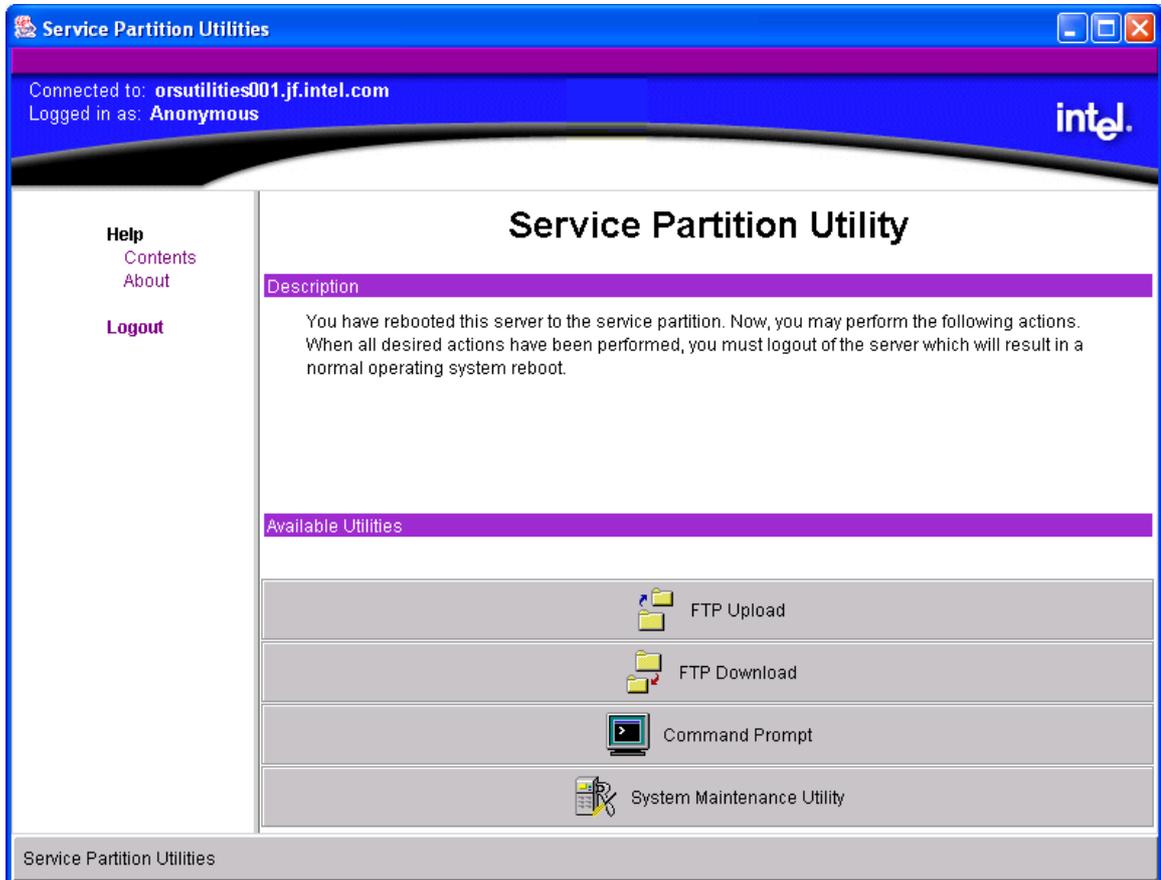
Figure 24. Service Partition Utilities

The remote SMU application attempts to establish a socket connection to the server and uses the Service Partition Utilities services to execute the server-side SMU core components. If a connection is established, the application sends information to the SMU core components to request a session. If the connection fails, a dialog box is displayed to indicate an error condition. In the event of an error, you can attempt to restart the SMU from the ISM console.

After the session with the SMU core components is established, a version check is made to determine if the remote SMU application is able to communicate with the SMU core components on the server. If the versions do not match, an error message is displayed, the SMU application is closed, and control is returned to the Service Partition Utilities application.

After the session between the SMU application and the core components is established, the window below is displayed. The primary information pane at the right directs you to select an activity from the task pane at the left.
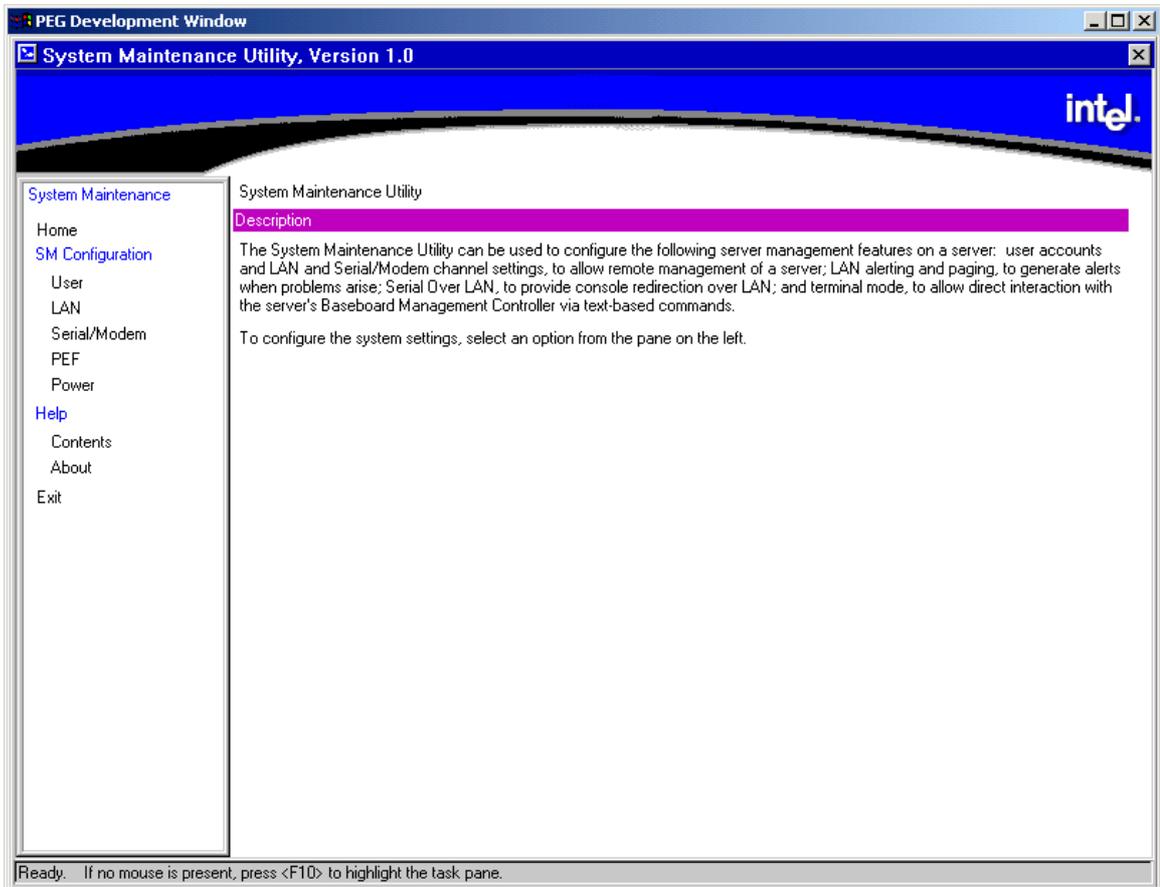
Figure 25. SMU Home

Local SMU Application

The local SMU application and the core components exchange XML documents using a procedural interface. There is no socket connection between the application and the core components.

The local SMU application can be run either from the system Resource CD or, if the SMU software has been installed locally, from the directory where it was installed on the system partition. The software can be run from a CD, regardless of whether it has been installed locally.

Running from CD

The target server must have a CD drive (EFI currently supports only CDs that contain information in the "El Torito" format). No network connection is required.

The following sequence of steps is followed to start the SMU locally (assuming the system Resource CD is being used):

1. Insert the system Resource CD into the CD drive on the target server and boot the server to the EFI shell. The Resource CD menu program begins running automatically and displays a splash screen followed by the main menu.
2. Use the arrow keys to move to the Utilities menu item. Press the `<Enter>` key.
3. Use the down arrow key to highlight the System Maintenance Utility menu item. Press the `<Enter>` key to start the local SMU application.

Running from the System Partition

To run the SMU application from a service partition on which it has been installed, follow the steps below:

1. If an EFI shell prompt is available on the local console and the files on the system partition can be accessed, skip to step 3.
2. Reset the server and boot to the EFI shell.
3. Locate the file system (e.g. fs0:, fs1:) that contains the service partition software and change directory to `\efi\service\smu`.
4. Run `smu.efi`.

Shutdown SMU Application

Exit either the local or remote SMU application by clicking on the Exit item in the task pane or by clicking the Close button in the upper right hand corner of the container. A user can also use the `Close` option in the system menu of either container. An exit operation can be started at any time (unless the application is blocked while it waits for a response from the server). During the exit process, the following steps occur:

1. The application sends a message to the SMU core components asking to end the SMU session.
2. The SMU core components send a message to the application asking for user confirmation of the exit request. This message is displayed as a dialog box with an `OK` button and a `Cancel` button.
3. Clicking the `OK` button causes the SMU application to send another message to the server to confirm the exit request. If `Cancel` is clicked, the request to close is canceled.
4. A final message is sent to the application from the server before the application shuts down. When the local SMU application is used, it exits to the EFI shell. When the remote SMU appliation is used, control is returned to the Service Partition Utilities application.

Server Management Configuration Task

The server management configuration task appears in the task pane of the SMU. This task allows you to configure server management settings maintained the Baseboard Management Controller. The server management configuration task supports configuring of the following, which are displayed as sub-tasks:

- LAN Channel
- Users
- Platform Event Filtering (PEF)
- Serial/Modem Channel
- Power Settings

Upon selecting one of the above sub-tasks, a screen is displayed that contains some or all of the configuration items that pertain to the selected sub-task. The data that is initially displayed is read from the server management controller of the server. You can update the settings and save them back to the server.

Sub-tasks can be made up of one or more screens, depending on the server management configuration settings you enabled. Buttons that are common to the server management configuration tasks are described in Table 16.

Table 16.   Common Buttons for Configuration Management Sub-tasks

Button	Description
Save	Causes the current values of the settings in the current sub-task to be stored in non-volatile memory on the server.
Edit	Causes a screen to be displayed that allows you to change settings related to a single entry in a table.

LAN Channel Configuration Sub-task

The LAN channel configuration sub-task allows you to modify settings related to the LAN channel. The initial screen for configuring the LAN channel is shown in the figure below. The configuration settings are described below the figure.

```
LAN Channel Configuration
Description
The settings below allow a LAN channel to be configured.
General Settings
                  Access Mode: [Always Available ▼]
          Privilege Level Limit: [Administrator      ▼]
IP Address
☐ Enable DHCP
             Host IP Address: [10.7.155.3        ]
               Subnet Mask: [255.255.255.0     ]
      Default Gateway IP Address: [10.7.155.251      ]
     Default Gateway MAC Address: [00-00-00-00-00-00 ]
☑ Automatically resolve Default Gateway MAC Address
      Backup Gateway IP Address: [0.0.0.0           ]
      Backup Gateway MAC Address: [00-00-00-00-00-00 ]
☑ Automatically resolve Backup Gateway MAC Address

                              [ Next > ]  [ Help ]
```

Figure 26. LAN Channel Configuration

After completing this screen, click `Next` to move to the next screen to continue this sub-task.

Default LAN Configuration Settings Set by the SMU

The SMU automatically configures some server management firmware settings. These are not displayed on the screen above, but are listed below. Before these settings are set by the SMU, you must click through each LAN configuration screen by clicking the `Next` button until you reach the `Save` button on the final LAN configuration screen.

- **Gratuitous ARPs may be enabled:** This setting allows the BMC to generate gratuitous ARPs, which provides a mechanism for IP devices to locate the hardware addresses of other devices on the local network. If the server has a valid IP address and the LAN channel is enabled for messaging (the access mode is not set to Disabled) or alerting, then gratuitous ARPs are enabled.
- **Authentication enables are enabled:** These bits define what types of authentication are enabled to authenticate messages sent to the BMC by users of different privilege levels. The SMU enables authentication of type straight password, MD2, MD5, and none.
- **User-level authentication is disabled:** The SMU disables user-level authentication so that if a user is attached with a privilege level of User, no authentication is done on messages sent to or from the BMC. This improves the session performance.

Access Mode

This drop-down box configures the access mode for the LAN channel. The available options are:

- **Always Available:** The channel is dedicated to communication with the BMC and is available during all system states (powered-down, powered-up, pre-boot, sleep, run-time, etc.).
- **Disabled:** The channel is not allowed to communicate with the BMC.

Privilege Level Limit

This drop-down box determines the maximum privilege level at which communication on the channel can take place. It is a global privilege level that takes precedence over user privilege levels. For example, if a channel privilege level is set to the user level then only user-level commands can be executed, regardless of the user privilege level.

The meanings of the different privilege levels are described below:

- **Callback:** Only commands needed to initiate a callback session are allowed. Although ISM software does not support callback as a connection mechanism, it is still a valid privilege level because it defines a set of BMC commands that can be executed by a user.
- **User:** Only "benign" commands are allowed. These are primarily commands that read data structures and retrieve status. Commands that can be used to alter BMC configuration, write data to the BMC or other management controllers, or perform system actions such as resets, power on/off, and watchdog activation are disallowed.
- **Operator:** All BMC commands are allowed, except for configuration commands that can change the behavior of the out-of-band interfaces. For example, Operator privilege does not allow the capability to disable individual channels, or to change user access privileges.
- **Administrator:** All BMC commands are allowed, including configuration commands. An adminstrator can execute configuration commands that would disable the channel that the Administrator is communicating over.

Enable DHCP

The Enable Dynamic Host Configuration Protocol (DHCP) check box enables / disables the dynamic host configuration protocol to allow the server to automatically assign the Host IP address, Default Gateway IP address and Subnet Mask. DHCP is enabled when the box is checked.

When this option is enabled, the Host IP Address, Subnet Mask, and Default Gateway IP Address edit boxes are disabled. The system must be reset before this setting takes effect.

Host IP Address

This edit box is for the logical or Internet address of the host. The IP address is required when DHCP is disabled. The IP address is entered as a dotted notation, such as 192.168.0.2.

Subnet Mask

The edit box is for the host's subnet mask. The server uses this to decide if alert destinations are in the local subnet or in another subnet relative to the client console. The Subnet Mask is required when DHCP is disabled. The Subnet Mask is entered as a dotted notation, such as 255.255.0.0.

Default Gateway IP Address

This edit box is for the IP address of the router used when the BMC sends a message or an alert to a system on a different subnet than the BMC is on. It is required when DHCP is disabled. The IP address is entered as a dotted notation, such as 192.168.0.2.

Default Gateway MAC Address

This edit box allows you to enter the MAC address of the default gateway router. The MAC address is entered as a series of six pairs of hex digits separated by dashes, such as 00-01-62-d0-3e-66. Alphabetic hex digits (a-f) can be entered in uppercase or lowercase. This edit box is disabled by default and is only activated if the check box for Automatically resolve Default Gateway MAC address is not checked. If the edit box is cleared (no address is supplied), a message is displayed asking that a valid address be entered. This edit box is disabled if DHCP is enabled.

Automatically Resolve Default Gateway MAC Address

This check box allows you to specify whether the BMC should automatically attempt to resolve the MAC address of the default gateway router. This box is checked by default unless the MAC address edit box appears to include a valid MAC address.

If this box is not checked, you must provide the MAC address in the Default Gateway MAC Address field.

When the OK button is clicked, the firmware attempts to resolve the gateway MAC address. If the BMC cannot resolve the address, the screen is redisplayed with the box unchecked and you are asked to provide the MAC address in the Default Gateway MAC Address field. If the screen is redisplayed due to a MAC address resolution issue, any user data previously entered, other than the MAC address information, remains in place.

This check box is disabled if DHCP is enabled.

Backup Gateway IP Address

This edit box allows you to enter the IP address of a backup gateway router. The IP address is entered as a dotted notation, such as 192.168.0.2.

Backup Gateway MAC Address

This edit box allows you to enter the MAC address of the backup gateway router. The MAC address is entered as a series of six pairs of hex digits separated by dashes, such as 00-01-62-d0-3e-66. Alphabetic hex digits (a-f) can be entered in uppercase or lowercase. This edit box is disabled by default and is only activated if the check box for Automatically resolve Backup Gateway MAC address is not checked. If the edit box is cleared (no address is supplied), a message is displayed asking that a valid address be entered. .

Automatically Resolve Backup Gateway MAC Address

This check box allows you to specify whether the BMC should automatically attempt to resolve the MAC address of the backup gateway router. This box is checked by default unless the MAC address edit box appears to include a valid MAC address.

If this box is not checked, you must provide the MAC address in the Backup Gateway MAC Address field.

When the OK button is clicked, the firmware attempts to resolve the gateway MAC address. If the BMC cannot resolve the address, the screen is redisplayed with the box unchecked and you are asked to provide the MAC address in the Backup Gateway MAC Address field. If the screen is redisplayed due to a MAC address resolution issue, any user data previously entered, other than the MAC address information, remains in place.

LAN Alert Configuration

The LAN Alert Configuration screen is displayed when you click `Next` from the LAN Channel Configuration screen. The LAN Alert Configuration screen shows all configured destination IP addresses for LAN alerts and their associated settings. If no IP addresses are configured as alert destinations, the `Edit` and `Delete` buttons are disabled.

Figure 27. LAN Alert Configuration

After completing this screen, click `Next` to move to the next screen to continue this sub-task.

Enable LAN Alerting

This check box is used to enable or disable alerts on the LAN channel.

SNMP Community String

This edit box is used to enter a string for Platform Event Traps (PETs). This field can optionally be used for a vendor-specific string that is used to provide the network name identity of the system that generated the event. This string is restricted to a maximum of 18 bytes and it is typically set to `public`. This string can be null.

Alert Settings

Up to four LAN alert destinations can be configured. When one or more IP addresses are configured as alert destinations, this part of the screen shows those addresses, along with the following associated configuration settings:

- Gateway IP address for the destination IP address.
- Whether alert acknowledge is enabled for the alerts sent to this destination.
- The number of times the alert will be retried.
- The interval in milliseconds between retries.

New, Edit, and Delete Buttons

If no alerts are configured, only the `New` button is enabled.

- New: When the `New` button is clicked, you are shown a screen on which you can configure a new LAN destination address. See the following section for details.
- Edit: If you select an IP address and then click the `Edit` button, you are shown a screen where you can edit the configuration for the selected IP address. See the following section for details.
- Delete: If you select an IP address and then click the `Delete` button, the selected IP address is deleted. Before deleting the IP address, you are prompted by a confirmation prompt. If you click `OK` to confirm deleting the address, the LAN Alerting Configuration screen is redisplayed with the deleted address no longer shown.

These buttons affect only the copy of the firmware data internal to the SMU; changes are written to non-volatile storage in the firmware only after you select the `Save` button in the last LAN configuration screen.

New/Edit LAN Alert

The New/Edit LAN Alert screen is displayed when you click either `New` or `Edit` on the LAN Alert Configuration screen. The New/Edit LAN alert screen allows you to configure or change the settings related to an IP address that is to receive alerts. The screen displayed either to configure a new alert destination or to edit an existing alert is the same, except that when editing an existing alert destination, the current settings read from the firmware are automatically displayed.

Figure 28. New / Edit LAN Alert

After completing this screen, click `OK` to return to the LAN Alert Configuration screen.

Destination IP Address

This edit box allows you to enter the IP address to which an alert is to be sent. The IP address is entered as a dotted notation, such as 192.168.0.2. The SMU does not check whether an IP address matches a previously entered address.

Destination MAC Address

This edit box is used to enter the MAC address of the destination machine to which the alert should be sent. This box is used when the destination IP address is outside the subnet that the server is on. The MAC address should be entered as a series of six pairs of hex digits separated by dashes, such as 00-01-62-d0-3e-66. Alphabetic hex digits (a-f) can be entered in uppercase or lowercase. This edit box is disabled by default and is only activated if the check box is not checked for Automatically resolve destination MAC address.

Automatically Resolve Destination MAC Address

This check box allows you to specify whether the BMC should automatically attempt to resolve the MAC address of the destination system. This box is checked by default unless the MAC address edit box appears to include a valid MAC address.

If this box is not checked, you must provide the MAC address in the Destination MAC Address field.

When the OK button is clicked, the firmware attempts to resolve the destination MAC address. If the BMC cannot resolve the address, the screen is redisplayed with the box unchecked and you are asked to provide the MAC address in the Destination Gateway MAC Address field. If the screen is redisplayed due to a MAC address resolution issue, any user data previously entered, other than the MAC address information, remains in place.

Number of Retries

This edit box allows you to enter the number of times to retry sending an alert to a given destination. If alert acknowledge is enabled, then retries are sent only when if a timeout occurs while waiting for the acknowledgement. If alert acknowledge is disabled, the number of retries is equal to the number of times an unacknowledged alert is sent out.

If the number of retries is set to 0, only a single attempt is made to send the alert. When a number greater than 0 is entered, the alert will be retried only if a timeout occurs while waiting for the acknowledgement.

The number of retries must between 0 and 7.

Retry Interval

This edit box is used to set the retry interval for sending an alert or to set the acknowledge timeout when Enable Alert Acknowledge is enabled. The value entered into this field is disregarded if Enable Alert Acknowledge is disabled.

The retry interval is in seconds, with a recommended value of 3 seconds. The retry value must be between 1 and 255.

Enable Alert Acknowledge

This check box should be checked if the destination IP address should send an acknowledgement when an alert is received. If this box is checked, then an alert is only assumed to have been successfully sent if an acknowledgement is received.

Use Default Gateway

This check box should be checked if the IP address entered as the default gateway IP address for the LAN channel on the first LAN configuration screen should be used as the gateway for this destination IP address. If this box is not checked, the backup gateway IP address is used as the gateway IP address.

Serial Over LAN Configuration

The Serial Over LAN screen is displayed after you click `Next` on the LAN Alert Configuration screen. The Serial Over LAN screen, shown in the following diagram, allows you to configure the operation of the serial over LAN capability of the BMC.

The SMU sets up the SOL configuration such that SOL packets do not have to be authenticated. This enhances the performance of an SOL session.

Figure 29. Serial Over LAN Configuration

After configuring the Serial Over LAN information, click `Save` to complete this sub-task.

Enable Serial Over LAN

This check box is used to enable or disable the serial over LAN capability.

SOL Privilege Level

This setting is used to select the minimum operating privilege level that is required to be able to activate SOL. The choices are `User`, `Operator`, and `Administrator`. For the best performance, `User` should be selected.

Number of Retries

This field sets the number of times that the BMC tries to resend a SOL message to a remote console.

The number of retries must between 0 and 7.

Retry Interval

This field sets the number of milliseconds that the BMC waits between trying to send SOL messages to a remote client.

The value entered must be between 0 and 2559. The SMU truncates the digit in the ones column from any input number because the firmware maintains this value in 10 millisecond intervals. Therefore, any value that is entered between 0 and 9 is displayed as 0.

Baud Rate

This field sets the baud rate at which serial data is transferred by the BMC when SOL is active. The choices are `Default IPMI`, `9600 bps`, `19.2 kbps`, `38.4 kbps`, `57.6`, and `115.2 kbps`. If `Default IPMI` is selected, the baud rate used is the rate currently set for BIOS serial redirection. When SOL is active, serial communication with the BMC always occurs with 8 data bits, no parity, 1 stop bit, and RTS/CTS (hardware) flow control.

User Configuration Sub-task

The User Configuration sub-task provides a way to configure the user access to the LAN and Serial/Modem channels. Up to four users are allowed. Some of the options presented in these screens depend on how the channels have been configured; therefore, the channels should be configured before you access these settings.

Sessions allow a framework for user authentication and allow multiple IPMI messaging streams on a single channel.

After clicking on the User Configuration sub-task, the screen displayed below is shown. This screen displays an entry for each possible user that can be configured. This screen shows:

- Whether a particular user is enabled or disabled for channel access
- Whether a password is set for the user
- The privilege level the user has for each of the available channels that supports sessions (users can only access channels that support sessions)
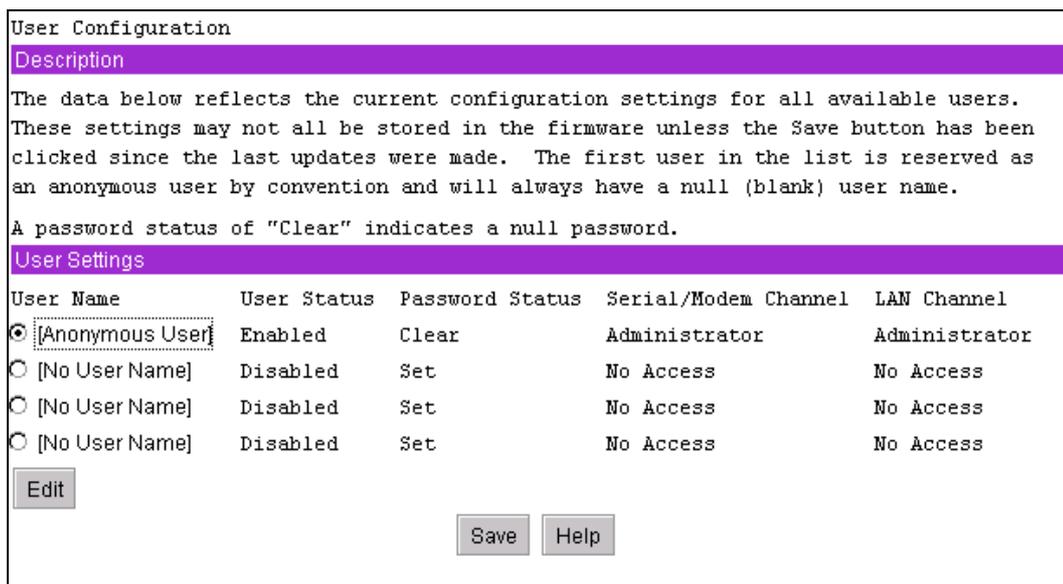
```
User Configuration
┌───────────────────────────────────────────────────────────────────────┐
│Description                                                              │
├───────────────────────────────────────────────────────────────────────┤
│The data below reflects the current configuration settings for all available users.│
│These settings may not all be stored in the firmware unless the Save button has been│
│clicked since the last updates were made.  The first user in the list is reserved as│
│an anonymous user by convention and will always have a null (blank) user name.│
│                                                                         │
│A password status of "Clear" indicates a null password.                  │
├───────────────────────────────────────────────────────────────────────┤
│User Settings                                                            │
└───────────────────────────────────────────────────────────────────────┘
User Name          User Status   Password Status   Serial/Modem Channel   LAN Channel
⊙ [Anonymous User]  Enabled       Clear             Administrator          Administrator
○ [No User Name]    Disabled      Set               No Access              No Access
○ [No User Name]    Disabled      Set               No Access              No Access
○ [No User Name]    Disabled      Set               No Access              No Access

  Edit

                              Save    Help
```

Figure 30. User Configuration

The first user is always present and is used to support an anonymous login. The username for this user is null (blank) and cannot be changed; the user name displays the text `Anonymous User`. The password can be set to a desired value.

It is possible for multiple user entries to have the same username. This occur is if a different password is needed for the same user on different channels. In this case, the privilege level for the channel that is not to be accessed with the associated password should be set to `No Access`. Otherwise, the firmware attempts to use the first entry in the user table that it finds

that allows access to the specified channel and would expect the password associated with that entry to be the one entered to gain access to the specified channel.

The figure below shows the screen that is displayed when a User Name is selected and then the `Edit` button is clicked. Changes made to user settings do not take affect until the next time that the user establishes a session.

After configuring the user information, click `Save` to complete this sub-task.

Figure 31. Edit User Configuration

After editing the user information, click `OK` to return to the User Configuration screen.

Enable User

This check box is used to enable you to attempt to have access to the available channels. Leaving the box unchecked disables the user, preventing that user from accessing the channels.

Enter Username

This edit box is used to enter an out-of-band username. If the anonymous user is selected for modification, the screen displayed does not include this edit box because the user name cannot be changed.

The password can be from 1 to 16 ASCII characters long. The characters accepted by the SMU for usernames are the ASCII printable characters in the range 0x21 through 0x7e, except for left and right bracket characters ('[' and ']'). These characters are reserved for framing packets for terminal mode sessions.

Clear Password

This check box is used to clear the password for the user. If this box is checked, the Enter and Verify New Password edit boxes are disabled.

Enter/Verify New Password

These edit boxes allow you to enter the password for the user. The Verify New Password edit box ensures that the password entered in the Enter New Password edit box is correct. As a user enters a password, asterisks are displayed. If a password already exists, these fields show `********` when you enter this screen.

This password can be between 1 and 16 ASCII characters in length. The characters accepted by the SMU for user passwords are the ASCII printable characters in the range 0x21 through 0x7e, except for left and right bracket characters (`[` and `]`), since those characters are used for framing packets for terminal mode sessions.

Note that if the `Clear Password` check box is checked, these two edit boxes are disabled.

If a user password is currently set, the SMU user is not required to enter the current password before changing it.

User Privilege Level for LAN Channels

This combo box allows you to select the privilege level for LAN channel. The global privilege level set for LAN channel access takes precedence over the user privilege level. For example, if the LAN channel is configured for user access only, then users are limited to user operations regardless of the user privilege level.

User Privilege Level for Serial/Modem Channel

This combo box allows you to select the privilege level for serial/modem channel access. The privilege level set for the serial/modem channel takes precedence over the user privilege level. For example, if the serial/modem channel is configured for user access only, then users are limited to user operations regardless of the user privilege level.

Platform Event Filtering (PEF) Sub-task

The Platform Event Filtering (PEF) sub-task provides a way to configure the BMC to take selected actions on event messages that it receives or has internally generated. These actions include operations such as system power-off and system reset, and triggering an alert message.

The BMC maintains an event filter table that is used to select the events that will trigger an action. Each time the BMC receives an internally or externally generated event message it compares the event data against the entries in the event filter table. If it finds a match, it performs the configured action(s).

The initial PEF sub-task screen is shown in the figure below.

Figure 32. Platform Event Filter Configuration

After completing this screen, click `Next` to move to the next screen to continue this sub-task.

Enable PEF

This option is used to globally enable or disable platform event filtering.

Enable SEL Event Messages for PEF Actions

When this option is checked, each action triggered by a filter generates an event message for the action. This allows the occurrence of PEF-triggered events to be logged in the System Event Log if event logging is enabled.

PEF Startup Delay

This option is used to configure the time in seconds to delay platform event filtering after a system power up or reset.

The number number of seconds allowed is between 60 and 255. The default is 60 seconds.

Alert Startup Delay

This setting is used to configure the time in seconds to delay sending out alerts after a system power up or reset.

The number number of seconds allowed is between 60 and 255. 0 indicates no delay.

PEF Action Global Settings

This set of check boxes globally enables PEF actions that can occur when an event filter is triggered. For a filter to trigger a particular chassis action (power cycle, reset, power down, or diagnostic interrupt) the global setting must be enabled and the specific chassis action must be selected for the filter. The chassis actions are configured in the screen that appears after you click `Next`.

The check boxes allow enabling or disabling of the following:

- **Power Cycle:** This check box globally enables / disables the Power Cycle action when an event filter is triggered. The action is enabled when the box is checked.
- **Reset:** This check box globally enables / disables the system reset action when an event filter is triggered. The action is enabled when the box is checked.
- **Power Down:** This check box globally enables / disables the system power down action when an event filter is triggered. The action is enabled when the box is checked.
- **Diagnostic Interrupt:** This check box globally enables / disables a diagnostic (non-maskable) interrupt when an event filter is triggered. The action is enabled with the box is checked.
- **Alert:** This check box globally enables / disables alerts when an event filter is triggered. The action is enabled when the box is checked.

Event Filter Settings

The PEF Event Filters Settings screen, shown in the figure below, displays the supported pre-configured event filters, along with settings associated with the event filters. These associated settings are:

- Whether the filter is enabled or disabled.
- The policy number associated with the filter (required only if alerts are enabled).
- A chassis action that occurs if the filter event occurs.
- Whether alerts are enabled or disabled if the filter event occurs.

The settings associated with a particular filter can be edited. Select the radio button next to a filter and then clicking the `Edit` button.

Figure 33. Event Filter Settings

If you click in one of the radio buttons and then click Edit, the Edit Event Filter Settings screen is displayed for the selected event filter. After completing this screen, click `Next` to move to the next screen to continue this sub-task.

Edit Event Filter Settings

The screen shown below is displayed after the `Edit` button is clicked on the Event Filters Settings screen.

Figure 34. Edit Event Filter Settings

After completing this screen, click `Ok` to return to the Event Filter Setting screen.

Enable Event Filter

The Enable Event Filter enable / disables the selected filter. The filter is enabled when the box is checked.

Enable Alerts

This check box causes an alert to be sent when an event associated with the selected event filter occurs. If the box is not checked, or if the global enable for alerts is not enabled, no alert is sent.

Policy Number Associated With This Event Filter

This drop-down box allows you to specify an alert policy number to be associated with the event filter. This setting is enabled only if the Enable Alerts box is checked; a valid policy number must be chosen if alerts are enabled.

The drop-down list shows the valid policy numbers, between 1 and 15. You will assign policy numbers to policy table entryies when you click the `Configure Policies` button.

Chassis Action Associated With This Event Filter

This drop-down box allows you to select the chassis action that is associated with the selected event filter. Chassis actions include power down, power cycle, reset, diagnostic interrupt, and none. For any chassis action to occur, it must be globally enabled on the Platform Event Filter Configuration screen.

Configure Policies Button

This button provides access to the screen that displays the current settings of all entries in the policy table, where you define the settings associated with the policy numbers used in the Policy number associated with this event filter drop-down box.

Alert Policy Table

The figure on the following page shows all the entries in the alert policy table, regardless of whether any settings are associated with a particular entry. All entries are shown because the entries in the table are order-dependent, so that when an alert occurs, entries in the table are processed from top to bottom as the firmware attempts to match table entries with the policy number associated with the event that caused the alert. By seeing all entries, you are able to ensure that the entries are in the correct order.

One use of the policy table is to be able to specify multiple destinations for alerts that occur. This can be done by assigning the same policy number to multiple entries in the table; but specifying different destinations in the destination field. If one policy is associated with multiple entries in the policy table, you can further refine the destinations that receive alerts by using the policy type.

Because the firmware goes through the table in order from top to bottom, when an event occurs, the table is searched in order for entries in which the policy number matches the policy number associated with the event filter. Therefore, the alert is sent to the destinations in the order in which they are encountered in the policy table. Make sure the destinations appear in the table in the desired order.

```
Alert Policy Configuration
Description
This view shows all of the entries in the alert policy table, including the
unconfigured entries.  Refer to the help for more information.
Policy Settings
Policy  Status    Policy  Channel              Destination
Number            Type
◉ 1    Enabled   A       LAN Channel          11.7.166.39
○ 1    Enabled   A       LAN Channel          11.7.155.12
○ 1    Disabled  A       LAN Channel          11.7.166.39
○ 1    Disabled  A       Serial/Modem Channel
○ 4    Disabled  A       LAN Channel          11.7.166.39
○ 1    Disabled  A       LAN Channel          11.7.166.39
○ 0    Disabled  A       Unknown
○ 1    Disabled  A       LAN Channel          11.7.166.39
○ 0    Disabled  A       Unknown
○ 4    Enabled   A       LAN Channel          11.7.166.39
○ 0    Disabled  A       Unknown
○ 0    Disabled  A       Unknown
○ 0    Disabled  A       Unknown
○ 0    Disabled  A       Unknown
○ 0    Disabled  A       Unknown
○ 0    Disabled  A       Unknown
○ 0    Disabled  A       Unknown
○ 0    Disabled  A       Unknown
○ 0    Disabled  A       Unknown
○ 0    Disabled  A       Unknown

  Edit

              < Back    Save    Help
```

Figure 35. Alert Policy Configuration

After completing this screen, click `Save` to complete this sub-task. The settings shown for each table entry are:

- Alert policy number
- Status indicating whether the table entry is enabled or disabled.
- Policy type determines how the firmware processes multiple entries that have the same policy number
- Channel on which the alert corresponding to the table entry would be sent.
- Destination IP address or phone number of the alert.

To edit a policy, click in the radio button next to the item and then click `Edit` to display the Edit Alert Policy Entry screen. After configuring the Alert Policy information, click `Save` to complete this sub-task.

Edit Alert Policy Entry

When you select an alert policy on the Alert Policy Configuration screen and then click the Edit button, you will see the Edit Alert Policy Entry screen, as shown below. Changes made on this screen apply to the alert policy selected when you clicked Edit.

After you click OK on this screen, you are returned to the Alert Policy Configuration screen

Figure 36. Edit Alert Policy Entry

After completing this screen, click Ok to return to the Alert Policy Configuration screen.

Enable Policy Entry

This check box enable / disables the selected policy table entry. If disabled, the firmware does not look at that table entry when attempting to match entries to the event that occurred. This option is enabled when the box is checked.

Policy Number

This edit box associates a policy number with a policy table entry. If the selected table entry is already associated with a policy number, that policy number is displayed. If a policy number is not associated with the selected table entry, 1 is displayed.

If alerts are associated with event filters, a valid policy number is required. Therefore, it is not possible to select 0 as a policy number.

Policy Type

This drop-down box displays a list of letters that represent the policies that can be associated with an alert policy table entry. The policy type determines how the firmware processes multiple entries in the policy table that have the same policy number. For example, the policy type can be used to indicate whether an alert is to be sent to multiple destinations or to destinations involving the same channel. The policy choices are listed below:

- **A**: Always send an alert to the destination referenced in this policy table entry.
- **B**: If the alert to the previous destination was successful, do not send an alert to the destination referenced in the current policy table entry. Instead, proceed to the next entry in the policy table that has the same policy number.

- **C**: If the alert to the previous destination was successful, do not send an alert to the destination referenced in the current policy table entry. Stop processing policy table entries.
- **D**: If the alert to the previous destination was successful, do not send an alert to the destination referenced in the current policy table entry. Instead, proceed to the next policy table entry that has the same policy number, but has a different channel destination.
- **E**: If the alert to the previous destination was successful, do not send an alert to the destination referenced in the current policy table entry. Instead, proceed to the next policy table entry with the same policy number that has a different destination type.

Select the Destination

This set of radio buttons shows the possible channel destinations that can be associated with a policy table entry. Each radio button is associated with a drop-down list of destinations that have been configured for that channel. Only the selection made in the drop-down list associated with the active radio button (channel) is used.

Serial/Modem Channel Configuration Sub-task

The serial/modem channel configuration sub-task allows you to modify settings that relate to the serial/modem channel, set up dial strings to which alerts are sent, and specify the settings related to sending alerts to those destinations.

This sub-task includes a screen that allows you to configure the settings for the terminal mode of operation of the serial/modem channel.

Figure 37. Serial / Modem Channel Configuration

After completing this screen, click `Next` to move to the next screen to continue this sub-task. The screen that is displayed when the `Next` button is clicked depends on which connection mode is chosen:

- If modem mode is selected, the next screen displayed allows setup of modem parameters
- If direct connect is selected, since there are no configuration parameters to set, the next screen displayed is the Destination Dial Strings screen.

Default Serial/Modem Configuration Settings Set By the SMU

The SMU sets some serial/modem configuration settings automatically. This information is listed below, but is not displayed on the screen. The list of these settings is given below. Before this information is set by the SMU, you must click through the remaining Serial/Modem Channel Configuration sub-task screens to click the `Save` button on the last screen.

- Authentication type enables are enabled. These bits define what types of authentication are enabled to authenticate messages sent to the BMC by users of different privilege levels. The SMU enables authentication of type straight password, MD2, MD5, and none.
- Basic mode is enabled, allowing basic serial communications to take place over the serial/modem channel.
- Session inactivity timeout is set to one minute.
- Session termination bits are enabled to enable ending of a serial/modem session if an inactivity timeout occurs or if DCD is lost.
- Flow control and baud rate are set for IPMI messaging (flow control is set to hardware flow control; the baud rate is set to 19.2 kbps).
- The multiplexor that determines who controls the serial connector has various default settings enabled and disabled.

Connection Mode

The connection mode determines the protocols used when performing IPMI messaging to the BMC. After selecting a connection mode, clicking on the `Next` button displays the screen for the selected mode.

- **Direct Connect Mode:** When Direct Connect Mode is selected, the client console and target server are connected by a null modem cable attached between the serial ports of each system.
- **Modem Mode:** When Modem Mode is selected, the client system establishes a connection to the target server using a modem. Each system must have a modem attached, and the user on the client system must have the dial string for the modem connected to the target server.

Access Mode

This option is used to configure the access mode for the Serial/Modem channel. The choices are:

- **Pre-boot only:** The Serial/Modem channel is available only out-of-band while the machine is powered-off and during POST until the boot process is initiated. This option is primarily used with serial port sharing where it may be desirable to ensure that the BMC does not control the serial port while the operating system is running. The Pre-boot only setting does not affect Serial/Modem alerting. If alerting is enabled and software does not handle the event, the BMC takes control of the port for the time that it takes to deliver the alert.
- **Always Available:** The channel is dedicated to communication with the BMC and is available during all system states (powered-down, powered-up, pre-boot, sleep, run-time, etc.).
- **Shared:** Shared is the same as Always Available, but the BIOS leaves the serial port available for software use.
- **Disabled:** The channel is not allowed to communicate with the BMC except for alerting.

Privilege Level Limit

This is the maximum privilege level that users can have on this channel. It restricts users of the channel to a set of BMC commands that can be issued at that privilege level. For example, if the channel privilege limit is configured with a maximum privilege level of Operator, and a user is configured to have Administrator privilege, that user can still only execute Operator level commands over this channel. See the *LAN Channel Configuration Sub-task*, on page 53 for a description of the privilege levels.

IPMI Messaging Communication Settings

These parameters are the global settings for IPMI messaging, which include Direct Connect and Modem modes. IPMI messaging always occurs with 8 bits/character, no parity, and 1 stop bit. The COM settings that can be configured are:

- **Flow Control:** This option sets how the flow of data is controlled. Available choices are `No Flow Control`, `CTS/RTS (hardware handshake)`, and `XON/XOFF`.
- **Baud Rate:** This option sets the maximum rate in bits per second at which the data can be transmitted through the serial port. Available baud rates are `9600`, `19200`, `38400`, `57600`, and `115200` bps. Support for baud rates higher than 19200 is optional and SMU will only display those that the BMC supports.
- **Enable Data Terminal Ready (DTR) Hang-up:** When DTR Hang-up is enabled, hang-up of a modem connection is based on when the DTR signal becomes inactive. When this is enabled, the modem settings Modem Hang-up and Escape Sequences are not used.

Modem Mode Configuration

If Modem Mode is chosen as the connection mode in Serial/Modem Channel Configuration screen and you click `Next`, the Modem Mode Configuration screen is displayed. This mode is for applications that connect to the server via an external modem. The Modem Mode Configuration screen is displayed below.

Figure 38. Modem Mode Configuration

After completing this screen, click `Next` to move to the next screen to continue this sub-task.

Modem Init String

Enter the ASCII string used to initialize the modem. This string is typically set to `ATE1Q0V1X4&D2&C1S0=0`. The string can be up to 64 ASCII characters long, including the termination character. The BMC automatically follows this string with an `<Enter>` character or carriage return.

Modem Escape Sequence

Enter the ASCII escape string to be sent to the modem before sending a command string. This string can be up to five characters long and is typically set to +++. If this field is left empty, the BMC uses +++. The modem escape sequence is not sent to the modem if DTR Hang-up is enabled on the initial *Serial/Modem Channel Configuration Sub-task* screen on page 70.

Hang-up Sequence

Enter the ASCII string that is sent to the modem to terminate the session. This string can be up to eight characters long is typically set to ATH. The BMC automatically follows this string with an <Enter> character when sending it to the modem. If this field is left empty, the BMC uses ATH. The hang-up sequence is not sent to the modem if DTR Hang-up is enabled on the initial *Serial/Modem Channel Configuration Sub-task* screen.

Dial Command

Enter the ASCII string for the modem string used to initiate a dial sequence with the modem. If this parameter is left empty, the BMC uses ATD.

Ring Duration

The Modem Ring Time setting specifies the time it takes the BMC to claim the serial connection after detecting the phone ringing while monitoring the Ring Indicator (RI) line. By configuring the Ring Duration, you can specify the amount of time that the BMC takes to switch the mux when RI is first detected. The ring duration and ring dead time have meaning only when the serial/modem channel access mode is set to shared.

The default values that are stored in firmware need to be adjusted for the phone in the region where the server/modem is located. The suggested ring duration for a US phone is 10000 ms.

The ring duration value should be entered in 500 ms increments; the SMU will round entries down to the nearest 500 ms. A value of 0 configures the BMC to switch the mux immediately on the first detected transition of RI.

Enter a value between 0 and 31509; be aware that the SMU rounds values down to the nearest 500 ms, so the maximum valued used is 31500.

Ring Dead Time

This setting allows you to specify the amount of time that the RI signal must be deasserted before the BMC determines that ringing has stopped. The ring duration and ring dead time have meaning only when the serial/modem channel access mode is set to shared.

The ring duration value should be entered in 500 ms increments and the SMU will round entries down to the nearest 500 ms. A value of 0 configures the BMC to switch the mux immediately on the first detected transition of RI. The value entered should reflect any dependencies on modem type, location of server, and the phone line carrier.

The default values that are stored in firmware need to be adjusted for the phone in the region where the server/modem is located. The suggested ring dead time for a US phone is 7000 ms.

Enter a value between 0 and 7999; be aware that the SMU rounds values down to the nearest 500 ms, so the maximum valued used is 7500.

Destination Dial Strings

The screen shown below displays the current setting of each destination dial string available on the target platform. For the NovaScale 4020 Server, up to six dial strings can be configured.

A dial string can be modified or cleared by selecting the corresponding radio button and then clicking on the `Edit` button.

Figure 39. Destination Dial Settings

After completing this screen, click `Next` to move to the next screen to continue this sub-task.

New, Edit, and Delete Buttons

If no dial strings are configured, only the `New` button is enabled.

- **New:** When the `New` button is clicked, you are shown a screen where you can configure a new dial string. See the following section for details.
- **Edit:** If you select a dial string and then click the `Edit` button, you are shown a screen where you can edit the selected dial string. See the following section for details.
- **Delete:** If you select a dial string and then click the `Delete` button, the selected dial string is deleted. Before deleting the dial string, you are prompted by a confirmation prompt. If you click `OK` to confirm deleting the dial string, the Destination Dial Strings screen is redisplayed with the deleted dial string no longer shown.

New/Edit Dial String

The New/Edit Dial String screen is displayed when you click either `New` or `Edit` on the Destination Dial Strings screen. The New/Edit Dial String screen allows you to configure or change the settings related to dial string to which alerts are to be sent. The screen displayed either to configure a new dial string or to edit an existing dial string is the same, except that when editing an existing dial string, the current settings for that dial string are displayed.

If a dial string is changed to null (cleared), then when the `OK` button is clicked, that entry in the dial string list displays as `Not Configured`.
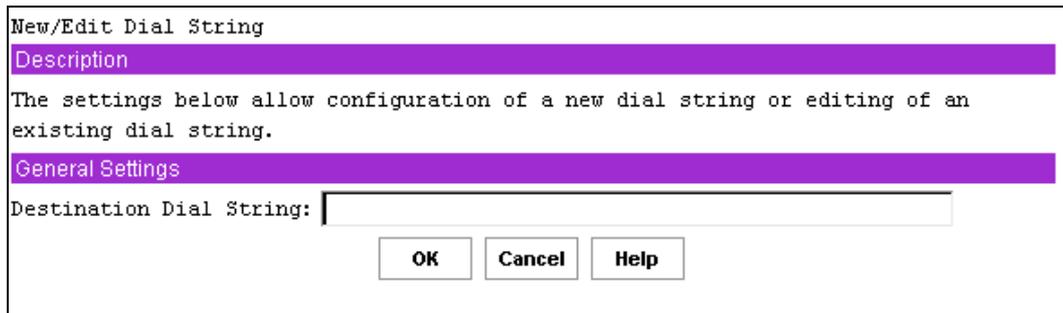
Figure 40. New / Edit Dial String

After completing this screen, click `OK` to return to the Destination Dial Strings screen.

Destination Dial String

When the BMC sends a dial string to a modem, it automatically precedes it with the currently defined Modem Init String sequence.

Valid dialing digits are `0-9`, `*`, `#`, A, B, C, D. The BMC can also recognize the following special characters:

- `P` – dial using pulse. Dialing digits following the `P` will be sent using pulse dialing.
- `T` – dial using tone. Dialing digits after the `T` will be sent using touch tones.
- `R` – reverse frequencies. Forces the modem to dial out at the answering frequency.
- `S=n` – dial a pre-stored phone number n.
- `W` – wait for dial tone.
- `@` - wait for quiet (answer).
- `,` `(comma)` – pause 2 seconds.
- `;` (Semi-colan) – return to command mode after dialing.
- `!` (exclamation point) – flash the switch hook

Page Destination Configuration

The Page Destination Configuration screen, shown below, is displayed when you click `Next` on the Destination Dial Strings screen. This screen allows you to configure the settings for each page destination that can be reached by sending a page through the serial/modem channel. Up to eight page destinations can be configured; the Dial String column displays `Not Configured` for any entry that has not been configured.

A page destination is comprised of:

- A dial string to be used when a page is to be sent out
- Retry information for the page
- Configuration of the modem at the destination

The data shown for each page destination includes the dial string, call retries, flow control, baud rate, parity, data bits, and stop bits for the destination modem. These settings are described in more detail in the next section. This screen also displays general settings that apply to all alerts to be sent as dial pages.

```
Page Destination Configuration
Description
This view shows all page destinations, configured or not.  From here, settings for
all page destinations can be modified.
General Settings
□ Enable Paging
            Page Blackout Interval: 0                              minutes
               Call Retry Interval: 60                             seconds
Page Destinations


Dial String        Call      Flow      Baud     Parity  Data   Stop
                   Retries   Control   Rate             Bits   Bits
⊙ 555555567        3         RTS/CTS   19200    None     7      1
○ [Not Configured] 3         None      19200    None     7      1
○ [Not Configured] 3         None      19200    None     7      1
○ [Not Configured] 3         None      19200    None     7      1
○ [Not Configured] 3         None      19200    None     7      1
○ [Not Configured] 3         None      19200    None     7      1
○ [Not Configured] 3         None      19200    None     7      1
○ [Not Configured] 3         None      19200    None     7      1
  Edit
                            < Back    Next >    Help
```

Figure 41. Page Destination Configuration

After completing this screen, click `Next` to move to the next screen to continue this sub-task. To configure or modify the settings for a page destination, select a radio button next to the entry and then click the `Edit` button to display the Edit Page Destination screen.

Enable Paging

This check box enables paging for the serial/modem channel.

Page Blackout Interval

The Page Blackout Interval determines the minimum number of minutes between pages. It provides a way to prevent back-to-back pages if a rapid series of events occurs. This parameter is entered in minutes; a value of 0 indicates no blackout.

Enter a value between 0 and 255.

Call Retry Interval

This setting gives the number of seconds between call retries when a busy signal is detected.

Enter a value between 0 and 255.

Edit Page Destination

When you select a Dial String on the Page Destination Configuration screen and then click `Edit`, you are shown the Edit Page Destination screen. On this screen, you configure or modify the settings for the selected page destination.

Figure 42. Edit Page Destination

After completing this screen, click `OK` to return to the Page Destination Configuration screen.

Dial String

This drop-down list shows all destination dial strings. The string selected before you clicked Edit on the Page Destination Configuration screen is displayed.

Flow Control

This drop-down configures the data flow control. Available choices are `No Flow Control`, `CTS/RTS` (hardware handshake), and `XON/XOFF`.

Baud Rate

This drop-down determines the maximum rate in bits per second at which the data can be transmitted through the serial port. Available baud rates are `9600`, `19200`, `38400`, `57600`, and `115200` bps.

Stop Bits

This drop-down determines the number of stop bits to use when transmitting page data. The choices are `1` or `2` stop bits.

Data Bits

This drop-down determines the number of data bits to use when transmitting page data. The choices are `7` or `8` data bits.

Parity

This drop-down determines the parity type that is used when transmitting the page data. The choices are `None`, `Odd`, or `Even`.

Call Retries

This edit box is the number of times to retry calling the destination specified by the destination dial string. A value of zero indicates no retries (the call is only made once).

Enter a value between 0 and 7.

Terminal Mode Configuration

When you click `Next` on the Page Destination Configuration screen, the Terminal Mode Configuration screen is displayed. This screen allows you to configure the settings used when terminal mode is active.

Terminal mode is an operating mode of the BMC in which the BMC can accept and respond to commands via printable characters over a serial/modem channel. This includes a set of text commands that the BMC understands and IPMI commands in hex format. For more information about Terminal Mode, see *Terminal Mode*, on page 106.

```
Terminal Mode Configuration
Description
The settings below allow the user to configure the terminal mode settings.
Terminal Mode Settings
☐ Enable Terminal Mode
☑ Enable Line Editing
Delete Control: Backspace ▼
☑ Turn BMC echo of received characters on
☑ Enable handshake when BMC ready to receive another message
Newline output sequence (BMC to console): CRLF ▼
Newline input sequence (console to BMC): CR ▼
                              < Back    Save    Help
```

Figure 43. Terminal Mode Configuration

After completing this screen, click `Save` to complete this sub-task.

Enable Terminal Mode

This check box enables or disables terminal mode. Terminal mode is enabled with the box is checked.

Enable Line Editing

This check box enables or disables line editing during a terminal mode session if checked. Line editing is enabled with the box is checked. When line editing is enabled, echo should also be enabled. When line editing is enabled:

- The `<Backspace>` or `<Delete>` key can be used to delete the last character entered.
- The `<ESC>` key can be used to delete an entire line.
- Long message lines can be split across multiple-lines using a line continuation (\) character followed immediately by `<CR><LF>`.

Delete Control

This drop-down box is enabled only if the Enable Line Editing box is checked. This option allows you to specify the delete control sequence for the BMC to use when `<Delete>` or `<Backspace>` is pressed. Users can choose from the following:

- The BMC outputs `<Delete>` when `<Backspace>` or `<Delete>` is received.
- The BMC outputs `<Backspace><Space><Backspace>` when `<Backspace>` or `<Delete>` is received.

Turn BMC Echo of Received Characters On

This check box allows you to enable or disable the BMC echoing characters it receives when in terminal mode. This feature is enabled when the box is checked.

Enable Handshake When BMC Ready To Receive Another Message

This setting enables or disables whether the BMC handshakes when ready to receive another message from you. When enabled, the BMC outputs the following string when it is ready to accept another message from the remote console:

`[SYS]<newline>`

Checking the box enables this feature.

Newline Output Sequence (BMC to console)

This setting allows you to select the characters that the BMC uses as a newline sequence when the BMC writes a line to the console when in terminal mode. The choices are

- `<CR><LF>`
- `<NULL>`
- `<CR>`
- `<LF><CR>`
- `<LF>`
- No termination sequence

Newline Input Sequence (console to BMC)

This setting allows you to select the characters the console uses as a newline sequence when writing to the BMC when the BMC is in terminal mode. The choices are

- `<CR>`
- `<NULL>`

Power Configuration Sub-task

The Power Configuration sub-task allows you to configure the power restore policy for the server. The power restore policy determines the action that the system takes when power is removed and then reapplied. This screen is shown below.
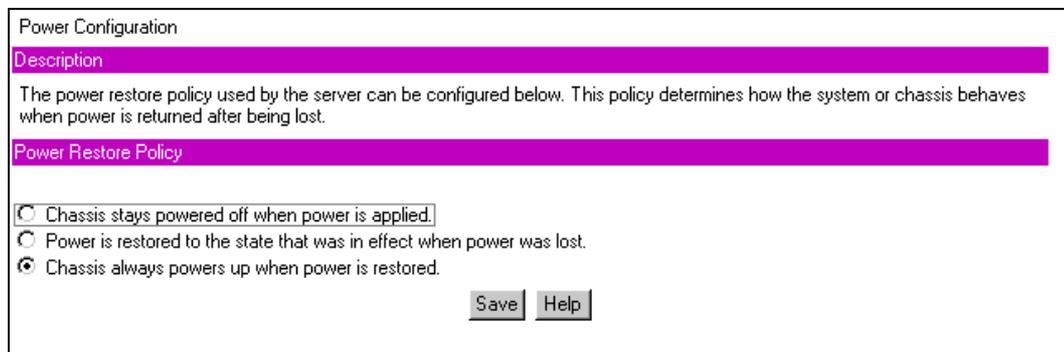
Figure 44. Power Configuration

After completing this screen, click `Save` to complete this sub-task.

The selected radio button is the current setting. However, it is possible for a policy value to be read from the firmware that does not correspond to any of these three settings. This value is classified as `unknown`. In this case, a dialog box informs you that such a state was read.

Chassis stays powered off when power is applied

When power is reapplied to the server, the server will not power up.

Power is restored to the state that was in effect when power was lost

If the system power was on when power was lost, the server will power back on. If the server was powered down, it will remain powered down when power is reapplied.

Chassis always powers up when power is restored

When power is reapplied, the server will power up.

SEL Viewer

NOTE

> The SEL Viewer task is available only on the local version of the SMU.
> This task is not available when running the remote version of the SMU.

The SEL Viewer task allows you to view the System Event Log. The SEL Viewer task supports the following:

- Viewing the BMC SEL
- Saving a log to a file
- Viewing a saved log file
- Viewing the SEL properties
- Clearing the BMC SEL

The SEL Viewer is started by clicking the SEL task in the task pane of the SMU. This task allows you to view the current system events logged in the SEL. Upon selecting the task, the entire SEL is loaded. During the load process, a dialog displays the progress. You cannot interrupt this process. After the load is completed you will see a warning message displayed if the SEL is full.

If the SEL is empty, the following message is displayed:

```
The SEL is empty, no records to display
```

After any messages have been dismissed, you will see a page of events. This page contains column headers and as many events that can fit on screen without using scroll bars. In order to prevent long display strings from creating scrollbars in the SEL Viewer the list view restricts the length of the following fields:

- Sensor Type and Number to 20 characters
- Event Description field to 30 characters
- Generator ID field to 15 characters

Viewing Events in the SEL

When the SEL Viewer is opened, the first page of events is loaded from the log and displayed. To view the remaining events you are provided with a series of buttons along the bottom of the screen. You can use the `<Tab>` key to access the screen buttons.
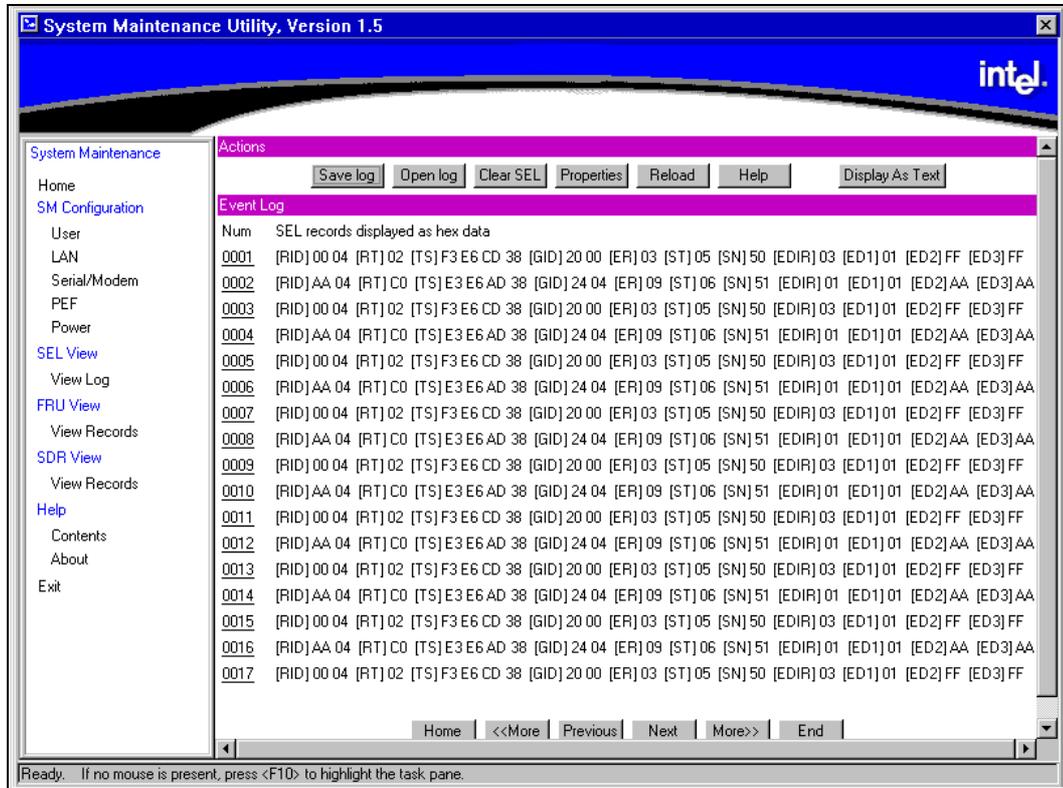
Acronym	Description
RID	Record ID
RT	Record Type
TS	Time Stamp
GID	Generator ID
ER	Event Message Format Revision
ST	Sensor Type
SN	Sensor Number
EDIR	Event Dir and Event Type
ED1	Event Data 1
ED2	Event Data 2
ED3	Event Data 3
MID	Manufacturer ID [1]
OEM	OEM defined [2]

Figure 45. SEL Viewer, Hex Display Mode

Home Button

The `Home` button displays the first segment of events. This button is disabled if the first event is displayed.

---

[1] Used when displaying OEM SEL Records Type C0h-DFh

[2] Used when displaying OEM SEL Records Type C0h-DFh and E0h-FFh

End Button

The `End` button displays the last segment of events. The number of events on this page varies based on the number of entries in the log; it may not fill the screen. This button is disabled if the last event is displayed.

Previous Button

This `Previous` button displays the prior segment of records. This button is disabled if the first event is displayed.

Next Button

This `Next` button displays the next segment of records. This button is disabled if the last event is displayed.

<<More Button

This `<<More` button backtracks by five segments of records. This is the equivalent of pressing the `Previous` button five times. If there are not five pages to backtrack, it goes to the first page of events. This button is disabled if the first event is displayed.

More>> Button

This button advances by five segments of records. This is the equivalent of pressing the `Next` button five times. If there are not five segments to advance through, it goes to the end segment. This button is disabled if the last event is displayed.

Viewing Single Events

Single events can be viewed in a modal popup window. The record to view is selected from the main screen by the link in the SEL ID field. The popup screen shows the hexadecimal view and the verbose text. The data is not limited in space, and no scrolling is required.

Sorting the SEL

The SEL can be sorted by clicking on the column header you wish to sort by. An arrow to the right of the column header indicates the sort-by column and whether the column is sorted in ascending or descending order. An up arrow indicates ascending order, and a down arrow indicates descending order. Clicking on the currently sorted column reverses the sort order of the column.

Whenever the SEL is sorted, the first segment is displayed.

Table 17.   SEL Sort Order Definitions

Sort Field	Ascending Order	Descending Order
SEL ID	Numeric ascending	Numeric descending
Time Stamp	Pre-Init time stamps first, followed by the most recent time stamp. Pre-init time stamps are sorted by SEL ID.	Most recent time stamp last, followed by the pre-Init time stamps. Pre-init time stamps are sorted by SEL ID.
Sensor Name	Alphabetic ascending	Alphabetic descending
Event Description	Alphabetic ascending	Alphabetic descending
Generator ID	Alphabetic ascending	Alphabetic descending

Save Log Button

This allows you to save the currently loaded SEL to a file. The user can choose to save the SEL as the decoded event data or as hexadecimal format. A different file extension is used for each type. In each case, the SEL properties and the entire log are written to the file. The SEL properties are saved at the top of the file and are saved as verbose text.

If the save fails because the file cannot be created, this error message is displayed:

```
Unable to create save file
```

If an error occurs while writing information to the file, this message is displayed:

```
Error saving SEL to the file
```

Open Log Button

This allows you to load a currently saved log file. The loaded file can be in either decoded or hexidecimal format. Upon opening a log file, the SEL Viewer is loaded, showing the events from the file.

If the file to open is not a valid SEL file, this message is displayed:

```
Invalid SEL file
```

If there is an error while reading the events from the file, this message is displayed:

```
Error reading SEL from file
```

If you load a hexadecimal log file, the viewer interprets data as if it was loaded from the system. You will have all of the functionality that is available when the data is loaded from the system, but the `Save Log` button is disabled when the log is loaded from a file.

Clear SEL Button

This allows you to clear all the system SEL events. Before proceeding with the clear, you are prompted with this message:

```
Do you really want to clear the SEL?  These events will be
permanently removed from the system
```

You are given two options with this prompt, `OK` and `Cancel`. Choosing `Cancel` will return you to the SEL Viewer main screen, choosing `OK` will clear the SEL. After the SEL is cleared, the log and properties are refreshed and the main screen is updated with the new SEL.

Properties Button

This shows you the current properties of the SEL. Included in the properties are:

- IPMI version
- Number of Entries
- Last Add Time
- Last Erase Time
- Free Space Remaining (both in bytes and number of SEL events)

A message is displayed if there is an error retrieving the SEL properties.

Reload Button

This button forces a refresh of the SEL from the system. Both the event list and the properties are refreshed.

Display as Hex Button

This button is only visible when the SEL is displayed in verbose mode. This will change the event display to Hex mode.

Display as Text Button

This button is only visible when the SEL is displayed in Hex mode. This will change the event display to text mode.

SDR Viewer

The SDR task allows you to view the current system SDR records stored in the BMC. It also provides the interface to opening and saving SDR files, and to viewing the SDR properties.

NOTE

> The SDR Viewer task is only available on the local version of the SMU. This task is not available when running the remote version of the application.

The SDR Viewer allows you to view the current BMC SDRs on the target system. The SDR Viewer task supports the following:

- Viewing the BMC SDRs
- Viewing the SDR properties.
- Saving the SDRs to a file
- Viewing a saved SDR file

When you select the SDR task, the SDRs are retrieved from the system. As the load progresses, a dialog window updates you on the status. You are not allowed to interrupt this process.

After the load is completed, a tree view of the system SDRs is displayed. The top branches of the tree are the SDR types. Under the branches are the records of that type. Clicking on the branch will expand and collapse it, showing or hiding the SDRs of that type. Clicking on an SDR will open a window that contains the SDR title, value, and byte location for each field in the record.

Only SDR types that have entries are included in the SDR tree view. If the viewer determines that a SDR record is invalid, the record is ignored and the remainder of the records are added to the tree. After the tree is created, a message box displays the following message if invalid records have been identified:

```
The SDR data read from the system contained invalid records,
these records will not be displayed by the viewer. Updating your
system's SDRs may correct this problem
```

If all the records are valid, no message is displayed. If there was an error retrieving the SDRs from the system, the following message is displayed:

```
Error retrieving SDRs from the system
```

An error message is also displayed if there was an error reading the SDR properties.

The SDR tree is navigable by using the keypad. The `<left arrow>` key collapses a branch if the current selection is on a branch. If the current selection is on a leaf, the selection is moved to the branch that contains the leaf.

The `<right arrow>` key expands a branch if the selection is currently on a branch. If the selection is not on a branch, there is no affect. The `<space bar>` and `<Enter>` keys have identical functionality, as follows: If the current selection is on a branch, an expanded branch collapses, and a collapsed branch expands. If the current selection is on a leaf, the SDR for that selection is shown in the SDR screen popup. No other keys affect the SDR tree.

The SDR tree retains its expanded/collapsed state for each of the branches until the SDRs are reloaded or until the application is exited. If the tree view goes beyond the size of the screen a vertical scroll bar is added to allow you to view all SDRs.

Viewing SDRs

SDR records can only be viewed one at a time. They are opened by clicking on the SDR in the SDR tree. No other actions are allowed once an SDR is opened for viewing. If the displayed data is too large to fit on the screen, the popup window is sized to the maximum viewable area and a vertical scroll bar is added. To view a new SDR or to issue another command, close the current window or use the `Next` and `Previous` buttons.
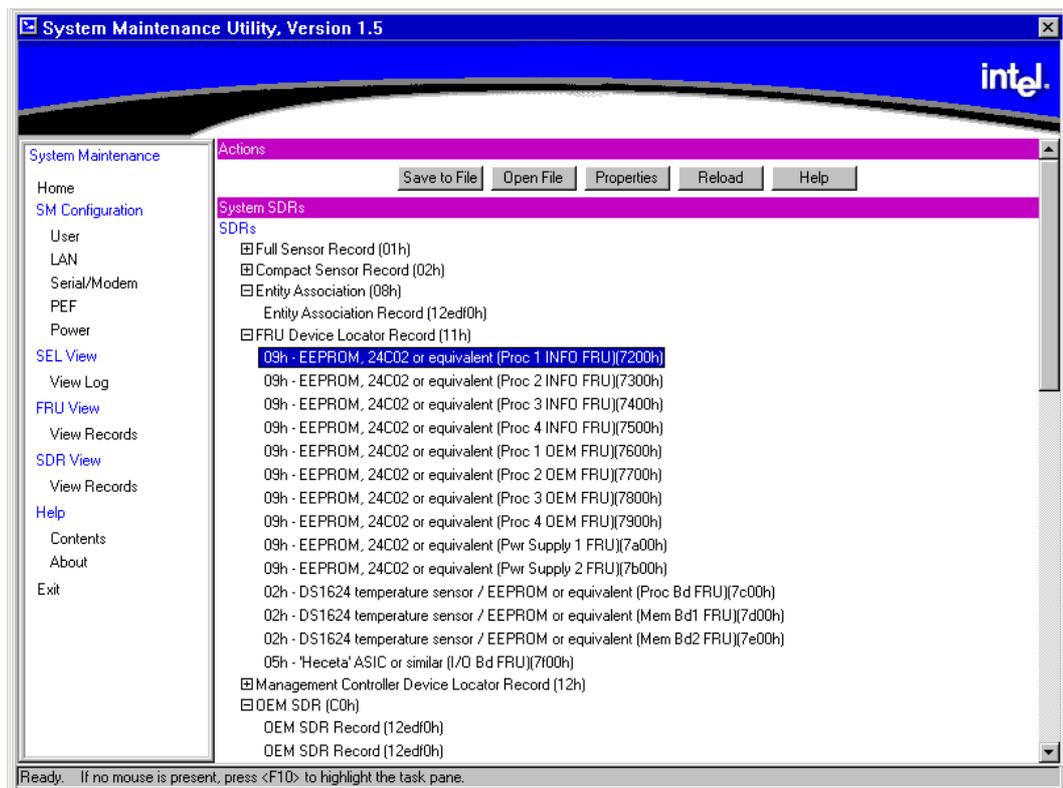
Figure 46. SDR Viewer

Individual SDRs of each type have their own display name format, as shown in the table below.

Table 18.   SDR Type Name Format

SDR Type [Hex]	Display Name Format
Type 1	[sensor type HEX] – [sensor type text] ([ID string]) sensor #[sensor number]
Type 2	[sensor type HEX] – [sensor type text] ([ID string]) sensor #[sensor number]
Type 8	[sensor type HEX] – [sensor type text] ([ID string])
Type 9	[sensor type HEX] – [sensor type text] ([ID string])
Type 10	[sensor type HEX] – [sensor type text] ([ID string])
Type 11	[sensor type HEX] – [sensor type text] ([ID string])
Type 12	[Entity ID HEX] – [entity ID text] ([ID string])
Type 13	[sensor type HEX] – [sensor type text] ([ID string])
Type 14	[sensor type HEX] – [sensor type text] ([ID string])
Type C0	*OEM SDR ([record ID])

The SDR type displays names in a single format: [SDR type hex] – [SDR type text] ([count of SDRs of this type]).

Under certain circumstances, the type C0 format does not follow the rules defined above. When all the characters of the data portion of the record are printable ASCII characters, the data area is considered to be a string and is used for the display name instead of the format defined in the table.

Close Button

This button closes the current SDR window and returns you to the SDR selection screen.

Previous Button

This button closes the current SDR window and displays the previous SDR record, the previous record must be of the same type as the current record. If this is the first SDR record in the SDR type branch, this button is disabled.

Next Button

This button closes the current popup window and displays the next SDR record in the SDR tree, the next record must be of the same type as the current record. If this is the last SDR record in the SDR type branch, this button is disabled.

Save To File Button

This button allows you to save the current SDRs to a file. If the save fails because the file cannot be created, the following message is displayed:

```
Unable to create save file
```

If an error occurs while writing information to the file, the following message is displayed:

```
Error saving SDRs to the file
```

Open File Button

This button allows you to open a currently saved SDR file. Upon selecting this option, all currently loaded SDRs are deleted and only the SDR loaded from the file are displayed. If the file is not a valid SDR file, an error message is displayed.

Properties Button

This button will force a refresh of the SDR properties and display them in a dialog. Included in the properties are: IPMI version, Number of SDRs, Last Add Time, Last Erase Time, and Free Space Remaining in bytes. If there is an error retrieving the SDR properties, an error message is displayed.

Reload Button

This button will clear the screen of the currently loaded SDRs and reload the SDRs from the BMC. This load procedure is identical to the load procedure that occurs when the viewer is opened.

FRU Viewer

The FRU Viewer sub-task allows you to view the current FRUs in the system.

NOTE

The FRU Viewer task is only available on the local version of the SMU. This task is not available when running the remote version.

The FRU Viewer allows you to view the current system FRUs on the target system. The FRU Viewer task supports the following:

- Viewing the current system FRUs
- Viewing the current system FRU properties.
- Saving the selected FRU to a file
- Viewing a saved FRU file

When you select the view records sub-task from the FRU menu, it immediately retrieves the system FRUs. In order to discover the system FRUs, the viewer must first scan the system SDRs and search the records for FRU locations.

After the scan of the SDRs is complete, the viewer starts loading the FRUs. If an error occurs while searching the SDRs, the viewer will try to load the FRUs based on the locator records found. The following error is displayed:

```
Error searching for FRU device locator records, not all FRUs may
be displayed. Updating your system's SDRs may correct this
problem
```

As the FRUs are loaded, a dialog window updates you with the progress. A progress window is updated for every FRU read. The message displayed is updated for each FRU.

After the FRUs are loaded, the FRU list and FRU area viewer are displayed. By default, the first FRU in the list is selected and displayed. If there is an error while retrieving the FRUs, the following message is displayed:

```
Error reading FRU at Device D Bus B ID I
```

`D`, `B`, and `I` are the values from the device locator record. This message will vary depending on the FRU type, but it will display sufficient information for you to display/update the FRU with the FRUSDR utility.

You are unable to stop either the FRU locator search or the FRU load process.

Viewing FRUs

To view a FRU, click on the FRU title in the FRU display list. The FRU board, chassis, and product areas are displayed on the right of the screen. If the area does not exist for the selected FRU, the following message is displayed for that area:

```
Not present
```

Only the displayable FRUs are in the list. The name that is used in the list is taken from the device locator record. If no displayable FRUs are present in the system, the title and value areas will contain the following message:

```
Not present
```

The FRU list is replaced by the message:

```
No Displayable FRUs present in system
```

The FRU that is currently being shown on the right side of the screen will appear as a string in the FRU list. It is not selectable.
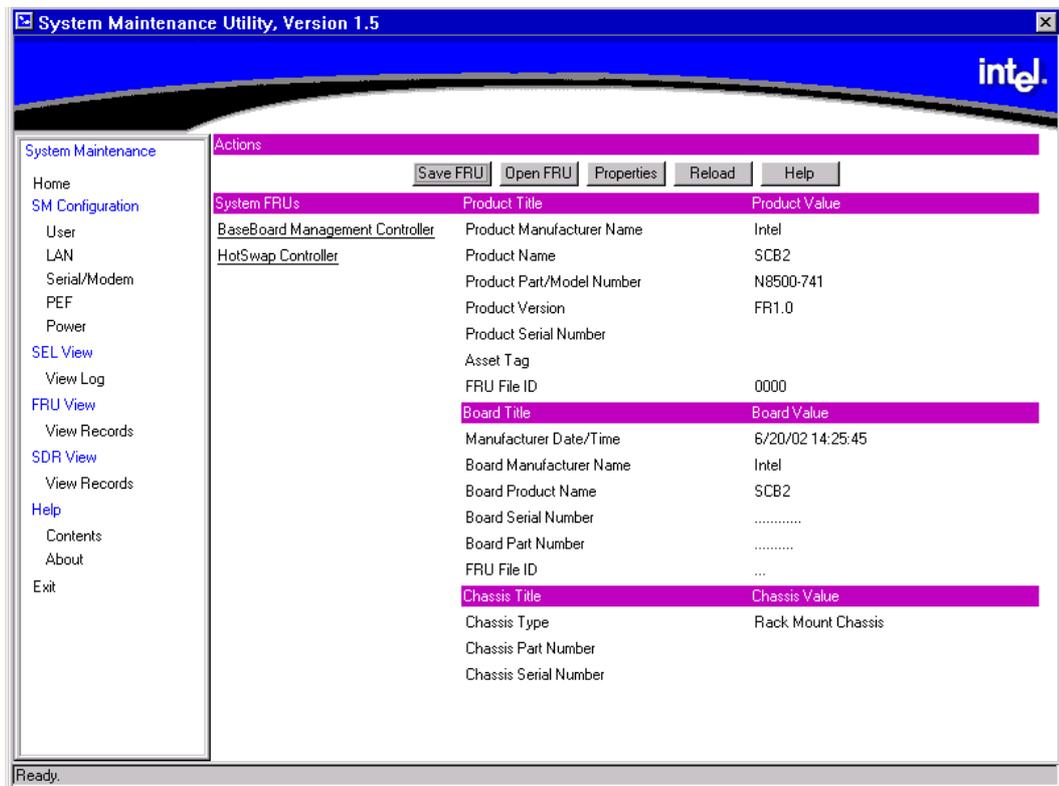

Figure 47. FRU Viewer

Save To File Button

This button allows you to save the currently displayed FRU to a file. If the save fails because the file cannot be created, this message is displayed:

```
Unable to create save file
```

If an error occurs while writing information to the file, this message is displayed:

```
Error saving the FRU data to the file
```

Open File Button

This button allows you to load a currently saved FRU file. Upon selecting this option, all currently loaded FRUs are deleted from the screen and the loaded FRU is displayed. If the file to open is not a valid FRU file, this message is displayed:

```
Invalid FRU file
```

If there is an error while reading the FRU from the file, this message is displayed:

```
Error reading FRU from file
```

Opening a FRU file will not affect the FRU properties.

Properties Button

This button will display the system FRU properties in a dialog. Included in the properties are: IPMI version, Number of FRUs in the system, and Number of IPMI formatted FRUs in the system. There is also a note to notify you that only IPMI formatted FRUs are displayed.

Reload Button

This will clear the currently loaded FRUs and refresh the FRUs from the system. This load procedure is identical to the load procedure when the viewer is opened.

Help Button

This displays the SMU context sensitive help for the FRU Viewer.

Task Error Handling

During the execution of a task, it is possible for errors to occur. These errors may be handled in different ways depending on the type of error. This chapter describes how error handling operates during SMU task execution.

Data Entry Errors

Some screens will ask for user input using edit boxes. In some of these boxes, the allowable user input needs to meet certain requirements, such as use of certain characters, a maximum length, or data within a particular range of values. The application does not check user input for validity; instead, when you click a button for the next screen, the current set of data is collected and sent to the SMU core components where it is checked. If a data entry error is found, a popup dialog box is displayed describing the error. In most cases the erroneous data is not cleared from the edit box in which it was entered. The user must clear the error and enter the correct information.

Internal Errors For Which a View Can Be Generated

Some errors may occur during task execution that result in an operation failing but are not fatal in that you can still attempt to perform other tasks. These types of errors include writing the server management settings to the BMC's non-volatile storage area, for example. In such a case, a screen is displayed containing information about the error that occurred and indicating whether or not you may attempt the operation again. These screens also have an OK button on them. When you click OK, the last screen displayed is redisplayed. You may also be informed as to whether the error was serious enough that you should shut down the SMU software or reboot the server.

Data Corruption Errors that the SMU Application can Handle

Data corruption errors that the SMU may be able to handle include corruption of template files used by the SMU (files that represent UI screens to be sent from the core components to the application). In this type of case, the SMU can detect that there is a problem when it is not able to correctly parse such a file, which means the application is not able to correctly display a screen. For this type of error, a message is displayed, indicating that a data corruption error has been encountered and that the current action cannot be completed. You are asked to select a new task from the task list.

Internal Errors For Which a View Cannot Be Generated

In a few cases, errors may be serious enough to prevent the SMU core components from supplying error information to you. These errors may include certain types of memory allocation errors or, in the remote case, the loss of the connection between the SMU application and the core components. In such cases, the SMU application (if possible), indicates to you that a shutdown of the software should occur and the server be rebooted.

Help

Help for the Remote SMU Application

Help for the remote SMU application is HTML-based. This means SMU help is displayed in a separate instance of a browser. See the figure below for a sample help screen.
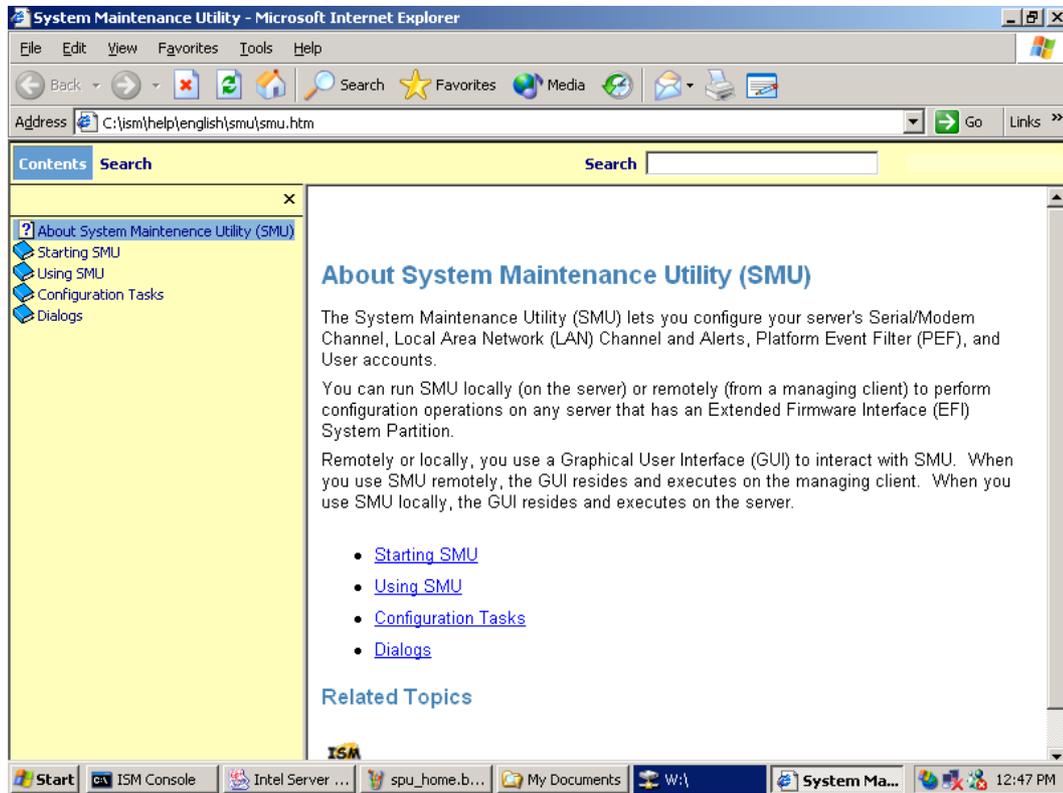
Figure 48. Remote SMU Help Window (browser based)

ISM Front-end Help

The front-end ISM help subsystem contains general information on the SMU. This help system does not provide details related to the screens displayed by the SMU. The ISM font-end help screens can be accessed by clicking on the Contents task in the task pane of the ISM Console.

SMU Table of Contents Help

After the SMU is launched, the SMU task pane provides a Help item with a Contents sub-task under it. You cannot click on the Help item itself, but when you click on Contents, a new browser window is launched. The Table of Contents pane at the left allows you to view context-sensitive help for any screen displayed by the SMU.

Each page displayed in the information pane at the right contains links labeled About SMU and ISM x.x Help, where x.x is the revision number of the ISM release. Clicking on About SMU returns you to a general front page for the SMU (is not context-specific). Clicking on ISM x.x Help launches a new browser that contains the front-end ISM help.

Most screens displayed by the SMU have a `Help` button. If no help is displayed, clicking `Help` launches a browser window that shows the context-sensitive help for the screen from

which you clicked `Help`; a table of contents is not displayed. If the link for About SMU link clicked, the help window is repainted with a table of contents pane and the About SMU information in the information pane. If the ISM x.x Help link is clicked, a separate browser window is launched and the front-end ISM help is displayed in that window.

If a help browser window was previously launched from the Contents task of the SMU application, then when a `Help` button on an SMU screen is clicked, the information pane is replaced with the context-sensitive help for the screen containing the `Help` button.

Help for the Local SMU Application

Help for the local SMU application appears in a modeless window on the client console. This means that when you want to return to the local SMU application, click on the application window to bring it to the foreground. You can use `<F1>` to toggle between the SMU application window and the help window. Since the application uses the entire screen and its container is not re-sizeable, the help window is hidden when the application window is brought to the front.

The help window is re-sizeable and can be moved. An example of the local help window is shown below.
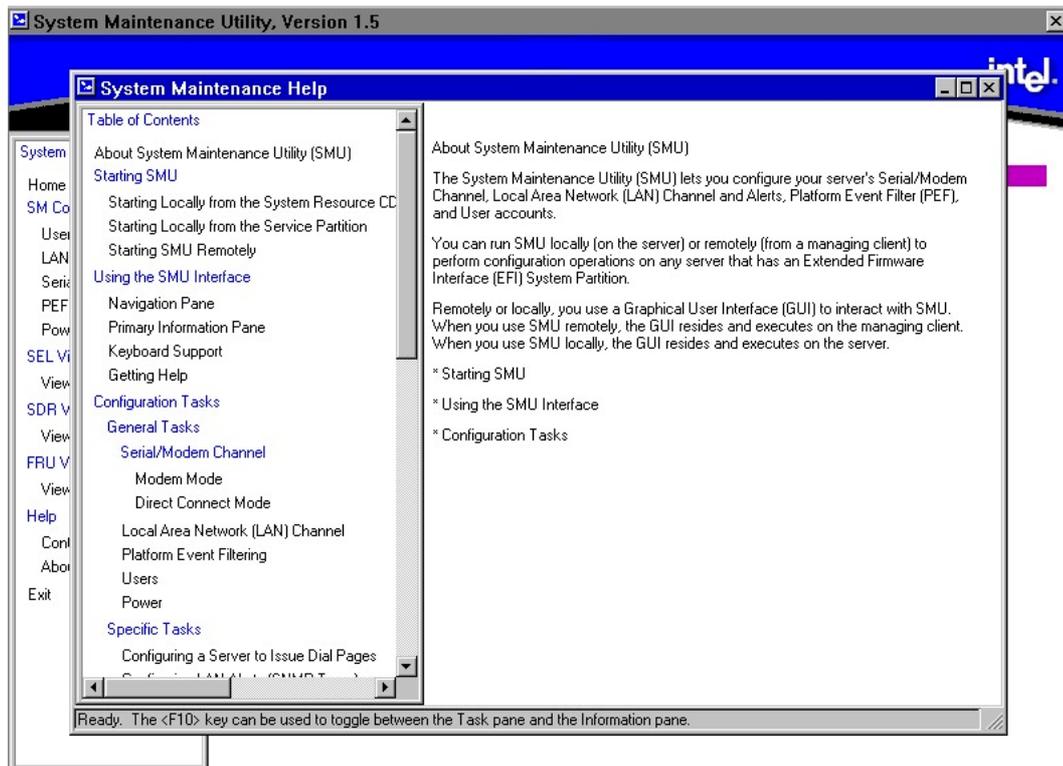
Figure 49. SMU Local Help Window

The Help window has a system menu that is available from the upper-left hand corner. This system menu allows you to minimize and maximize the Help window. The Help window also has minimize, maximize, and close buttons in the upper right corner. The task pane of the help window can be resized and displays horizontal and vertical scroll bars when necessary.

The information shown in the help window is obtained by running the HTML version of the help through a translator. Therefore, while the content is the same, the appearance is different because the local SMU application is not as flexible as a browser.

Most individual screens displayed in the primary information pane have `Help` buttons. Clicking a `Help` button causes the help that is related to that screen to be displayed in the help window, with the help window appearing in the foreground.

If the Help window is minimized it can only be redisplayed by pressing the `<F1>` key or clicking a `Help` button. If the Help window is not active and the `<F1>` key is pressed, the About SMU screen is displayed in the information pane. In general, all keys described in the section on local SMU keyboard support work for the help window as well as the local SMU application container.

EFI Platform Diagnostic Tests

EFI Platform Diagnostic Tests allow you to quickly assess the server's hardware status, view test logs, and determine the server's current configuration. You can run EFI Platform Diagnostic Tests from within the EFI environment.

Starting the Application

Use the following steps to setup and run tests.

> **NOTE**
>
> You can also run this utility from the Resource CD. This causes the utility to run in a RAM drive which means log files are volatile and will need to be copied to write-able media if they need to be saved.

1. Boot to the EFI shell.
2. Create the following directory on the target drive such as a hard drive:
   `efi\service\diagnostics`
3. Copy the distributed FieldDiags binary file (`fielddiags.efi`) to the root directory of the target.
4. Run the following command to unpack and install the FieldDiags software:

   `fielddiags -d \efi\service\diagnostics`
5. With your working directory on the same drive that contains the test software, type the following command to load and run the tests:

   `\efi\service\diagnostics\fielddiags`

   As an option, you can include a relative pathname in the command, based on your current working directory.

In addition to running tests, you can display system configuration information or the current test log. To do either, highlight the appropriate option and press the `<Enter>` key.

Understanding the General User Interface

The platform diagnostics application uses multiple screens from which you can choose execution options, enable or disable tests for execution, and define test parameters. The initial screen consists of four pull-down menus:

- File
- System Information
- Platform Test
- Help

The `<up-arrow>` and `<down-arrow>` keys navigate vertically through all areas of the screen. During navigation, items that you can modify become highlighted. `<Left-arrow>` and `<right-arrow>` keys navigate horizontally through the menus.

- Pressing the `<Enter>` key with an execution option highlighted causes the action to occur.
- Pressing the `<Enter>` key from within a dialog box causes data to be entered.
- Pressing the `<F1>` key while a test is highlighted or has the greater-than character (>) to the left of it causes on-line help for that test to appear.
- Pressing the `<ESC>` key with on-line help displayed or with a dialog box displayed dismisses the information or dialog box.

Understanding Basic Testing

The Platform Test menu is set up in the order that is typically used:

- Test Setup allows you to determine which tests to run and how thoroughly to test.
- Run Test starts test execution and provides some indication of test progress.
- View Results shows the results window and allows you to view and clear the test log.

Enabling Tests For Execution

To enable one or more tests for execution, select `Test setup` from the Platform Test menu. Use the `<up-arrow>`and `<down-arrow>`arrows to first select a test, and then press:

- `<Q>` for a quick test
- `<C>` for a complete test
- `<D>` to disable the test.

When a test is enabled, `Quick` or `Complete` appears next to the test under the `Coverage` column. If a test is disabled, the `Disabled` appears under that column. An individual test can be executed up to nine times for each run of the test suite. With the test highlighted, use the number keys to set the number of iterations for an individual test.

The test area of the screen displays six tests at a time. Use the arrow keys to scroll through the list.

NOTE

By default on startup all tests are set to quick test and single iteration.
You may go directly to `Run Test` if no changes are required.

Setting Test Options

The `Test` options pull-down menu opens the Test Options window. In the Test Options window you can determine if the test stops on one of two parameters; time or iterations. If you navigate to the Stop On item in the window and press the `<Enter>` key you are given the options of `Iterations` or `Minutes`:

- If `Iterations` is selected, the test suite repeats until it has completed the number of iterations indicated by the number in the `Iterations` edit box.
- If `Minutes` is selected, the test suite repeats until the number of minutes in the `Minutes` edit box has passed.

Interpreting Results

Test results appear next to the enabled tests in the test area of the screen. Each time a test passes or fails during a loop, the pass or fail count increments. For failed tests, Field Replaceable Unit information also appears under the `Details` column.

If you want greater detail for the test run, view the test log file. For information on how to view the test log file, refer to *Viewing the Test Log* below.

Help On Individual Tests

To display on-line help text files for a particular test, use the arrow keys to highlight the desired test and then press the `<F1>` key. You will see a scrollable text file that describes the sub-tests for the highlighted test.

Viewing System Information

To view system information, use the arrow keys to highlight the menu item, and press the `<Enter>` key. From the menu select the system information to be viewed.

After pressing the `<Enter>` key, you will see a scrollable information box that contains system information.

Viewing the Test Log

By default, the diagnostic software keeps the log file in `efi\service\diagnostics\fielddiags.log`.

To view this file, use the arrow keys to highlight the Platform Test menu. Select `View Results`, and press the `<Enter>` key. You will see a scrollable information box that contains the sessions test log. Because the log file is a Unicode file, you can also view it in the EFI shell by using the `type` -u command, and in the Windows operating system using the Notepad application.

Test results are appended to the previous log file. To clear the log file select the `Clear log` button in the View Results window. Because the log file is always appended, you should clear the file regularly to keep it from geting too large.

EFI Service Partition

The EFI Service Partition provides the ability to remotely access an Intel® server running EFI, via modem or LAN. This provides a way to execute configuration/setup utilities, and run remote diagnostics and other software designed to be compatible with this environment.

Service Partition Requirements

The SP may reside on any of the EFI-recognized physical drives. Drives not supported by EFI cannot be used for a service partition or EFI System Partition. An EFI System Partition cannot be installed on legacy MBR disks. The disk must be formatted as a GPT (GUID Partition Table) disk.

The SP requires at least 65 MB free on the chosen EFI System Partition and, for proper operation, there must be only one set of service partition files present.

Installing Service Partition Files

The service partition on an Intel Itanium 2-based platform is part of the EFI System Partition. This partition is not a separate, dedicated partition as is its functional counterpart on an IA-32 platform. The presence of service partition files within the existing system partition defines the EFI Service Partition.

The service partition is established when the installation program copies service partition files into the existing system partition. These files include utilities, diagnostics, and other software required for remote management. You can run the utilities and diagnostics located on the service partition either locally or remotely, but in order to run the utilities and diagnostics, you must boot the server from the partition. Applications that execute in the service partition run only on the managed server.

Installation Requirements

Adhere to the following requirements when installing the service partition files:

- The current ECO BIOS and Firmware are installed.
- Use the installation software on the current System Resource CD or software obtained from your Bull field representative.
- At least 125 MB or one percent of the selected drive must be available as un-partitioned space.

Installing the Files

Follow these steps to install the service partition files onto a managed server whose operating system is already installed:

1. Insert the System Resource CD into the managed server's CD-ROM drive. Alternatively, you can obtain the software from your Intel field representative. If you do so, follow the instructions included with the software package to install the service partition.
2. Boot the system into the EFI Shell; the EFI CD menu program launches automatically. If the EFI CD menu program does not launch in the EFI Shell, mount and map to the CD drive, type `startup`, and press `<Enter>`.

3. From the menu tab, use the arrow keys to navigate to the Utility menu and press `<Enter>` or the use the `<down arrow>` to expand the menu.

4. From the Utility menu, arrow to `Install Service Partition` and press `<Enter>` to launch the Service Partition Administration menu.

5. Choose `3` and press `<Enter>` to install the service partition files.

6. The installation software reports whether a system partition has been found. If so, it is recommended that you install the service partition files onto the existing system partition. Do so by choosing `1` and pressing `<Enter>`.

7. Choose the number for the system partition on which to install the partition files and press `<Enter>`.

8. After receiving the message indicating that all files were installed successfully, press any key.

9. Press `<ESC>` to exit the Service Partition Administration menu and return to the EFI CD menu.

Booting from the Service Partition

The service partition contains utilities and diagnostics. To run these utilities or diagnostics, you need to boot the server from the service partition. You can reboot a managed server from the service partition either locally or remotely. When you reboot the server to the service partition remotely, you can do the following:

- Run EFI shell commands on the server
- Run a program from the service partition
- Run diagnostics specific to the server
- Run the SMU to configure the server for Server Management

Locally

Follow these steps to locally boot the server to the service partition:

1. Restart the managed server.
2. Monitor the boot process and press `<F2>` when prompted to enter BIOS setup.
3. Arrow to the System Management menu, and select `Enabled` for the Service Boot option.
4. Press `<F10>` to save the setting and exit out of the BIOS setup. The system automatically reboots to the Service Partition.

Console Redirection

The BIOS supports redirection of video output and keyboard input via serial link. This section details the serial redirection scheme. For redirection over LAN (Serial over LAN or SOL), see the ISM online help.

When console redirection is enabled, local (host server) keyboard input and video output are passed both to the local keyboard and video connections, and to the remote console via the serial link. Keyboard inputs from both sources are considered valid and video is displayed to both outputs.

With console redirection, you can operate the server system without having a keyboard or monitor attached to it. Setup and any other text-based utilities can be accessed via console redirection. Note that serial redirection uses PC-ANSI and the UART settings assume 1 stop bit.

Operation

NOTE

When console redirection is enabled, the text on the local console screen will draw slowly when it is operating under EFI. This is especially true when a low baud-rate modem is used, such as the default baud rate of 19.2K. This is because EFI is not an interrupt-driven environment and it uses a polling mechanism to communicate with the remote console.

When redirecting through a modem, as opposed to a null modem cable, the modem needs to be configured as follows:

- Auto-answer (for example, `ATS0=2`, to answer after two rings).
- Modem reaction to DTR set to return to command state (such as `AT&D1`). Failure to provide the modem reaction results in the modem either dropping the link when the server reboots (as in `AT&D0`) or becoming unresponsive to server baud rate changes (as in `AT&D2`).
- The Setup/EMP option for handshaking must be set to `CTS/RTS + CD` for optimum performance. The CD refers to carrier detect. If the EMP is sharing the COM port with serial redirection, the handshaking must be set to `CTS/RTS+ CD`. In selecting this form of handshaking, the server is prevented from sending video updates to a modem that is not connected to a remote modem. If this is not selected, video update data being sent to the modem inhibits many modems from answering an incoming call. An EMP option utilizing CD should not be used if a modem is not used and the CD is not connected.

Once console redirection is selected via Setup, redirection binary is loaded into memory and activated during POST. While redirection cannot be removed without rebooting, it can be inhibited and restarted.

Inhibiting and restarting is accomplished through an INT 16h mechanism. The standard INT 16h (keyboard handler) function ah=05h places a keystroke in the key buffer, as if an actual key is pressed. Keystrokes buffered this way are examined by redirection; if a valid command string has been sent, it is executed. The following commands are supported:

- `Esc-CDZ0` - Inhibit Console Redirection. In order to inhibit redirection, the software must call INT 16h, function ah=05h five times to place the five keys in the key buffer. Keystrokes sent to the INT 16h buffers to invoking a command are buffered, and should be removed through normal INT 16h calls to prevent these keystrokes from being passed to

another application. When redirection is inhibited, the serial port is released and can be used by other applications.

- `Esc-CDZ1` - Restart Console Redirection. Restarting reclaims the serial port and continues redirection

Keystroke Mappings

During console redirection, the remote terminal sends keystrokes to the local server. The local server passes video back over this same link.

For keys that have an ASCII mapping, such as `<A>` and `<Ctrl><A>,` the remote sends the ASCII character. For keys that do not have an ASCII mapping, such as `<F1>` and `<Alt><A>`, the remote sends a string of characters, as defined in the tables below. The strings are based on the ANSI terminal standard. Since the ANSI terminal standard does not define all the keys on the standard 101 key U.S. keyboard, such as `<F5>`-`<F12>`, `<Page Up>`, and `<Page Down>`, mappings for these keys are available.

`<Alt>` key combinations are created by sending the combination `^[}` followed by the character to be `<Alt>` modified. Once this Alt key combination is sent, the next keystroke sent is translated into its `<Alt>`-key mapping. In other words, if is mapped to `<Shift><F1>`, then pressing `<Shift><F1>` followed by `^[}` sends `<Alt><a>` to the server.

The remote terminal can force a refresh of its video by sending `^[}`.

Combinations outside of the ANSI mapping and not in the table below, such as `<Ctrl><F1>`, are not supported.

Table 19.   Non-ASCII Key Mappings

Key	Normal	Shift	Ctrl	Alt
ESC	^[	NS	NS	NS
F1	^[OP	NS	NS	NS
F2	^[OQ	NS	NS	NS
F3	^[OR	NS	NS	NS
F4	^[OS	NS	NS	NS
F5	^[OT	NS	NS	NS
F6	^[OU	NS	NS	NS
F7	^[OV	NS	NS	NS
F8	^[OW	NS	NS	NS
F9	^[OX	NS	NS	NS
F10	^[OY	NS	NS	NS
F11	^[OZ	NS	NS	NS
F12	^[O1	NS	NS	NS
Print Screen	NS	NS	NS	NS
Scroll Lock	NS	NS	NS	NS
Pause	NS	NS	NS	NS
Insert	^[[L	NS	NS	NS
Delete	(7Fh)	NS	NS	NS
Home	^[[H	NS	NS	NS
End	^[[K	NS	NS	NS
Pg Up	^[[M	NS	NS	NS
Pg Down	^[[2J	NS	NS	NS
Up Arrow	^[[A	NS	NS	NS
Down Arrow	^[[B	NS	NS	NS
Right Arrow	^[[C	NS	NS	NS
Left Arrow	^[[D	NS	NS	NS
Tab	(09h)	NS	NS	NS

NS = Not supported

(xxh) = ASCII character xx

Table 20.   ASCII Key Mappings

Key	Normal	Shift	Ctrl	Alt
Backspace	(08h)	(08h)	(7Fh)	^[}(08h)
(accent) `	`	(tilde) ~	NS	^[}`
1	1	!	NS	^[}1
2	2	@	NS	^[}2
3	3	#	NS	^[}3
4	4	$	NS	^[}4
5	5	%	NS	^[}5
6	6	^	NS	^[}6
7	7	&	NS	^[}7
8	8	*	NS	^[}8
9	9	(	NS	^[}9
0	0	)	NS	^[}0
(dash) -	-	(under) _	(1Fh)	^[}-
=	=	+	NS	^[}=
a to z	a to z	A to Z	(01h) to (1Ah)	^[}a to ^[}z
[	[	{	(1Bh)	^[}[
]	]	}	(1Dh)	^[}]
\	\	|	(1Ch)	^[}\
(semi-colon) ;	;	(colon) :	NS	^[};
(apostrophe) '	'	(quote) "	NS	^[}'
(comma) ,	,	<	NS	^[},
(period) .	.	>	NS	^[}.
/	/	?	NS	^[}/
(space)	(20h)	(20h)	(20h)	^[}(20h)

NS = not supported

(xxh) = ASCII character xx

Limitations

Console redirection is a real-mode BIOS extension and has been modified to transition into EFI space. The transition is actually a parameter-passing exercise whereby the serial redirection scheme native to the EFI takes over using the settings established in BIOS Setup.

Video is redirected by scanning for, and sending changes to, text video memory across the redirection channel. Therefore, console redirection cannot redirect video in graphics mode. Keyboard redirection operates through the BIOS INT 16h handler. Software that bypasses this handler does not receive redirected keystrokes. After entering EFI, the redirection scheme changes somewhat, but the effect is the same.

Server Management Interface

The BIOS determines if console redirection is enabled, reads the current baud rate from the EMP, and passes this value to the appropriate management controller via the IPMB.

Sample Setup for Console Redirection

The following is an example of how to configure the console/host and server for BIOS console redirection. For Serial over LAN (SOL) console redirection, refer to the ISM documentation included on the ISM CD. In the example below, the console is running Windows* XP with SP3. The console and server are directly connected through the serial ports of both systems, using a null modem cable:

Server Configuration
1. Power on the server and when prompted, press the `<F2>` key to enter BIOS Setup.
2. The BIOS Setup menu displays the Main menu. Use the arrow keys move to the System Management menu.
3. At System Management menu, arrow to the Console Redirection submenu and press `<Enter>`.
4. Arrow to the `Serial Console Redirection` and press `<Enter>`.
5. Use the arrow key to select `Enabled` and press `<Enter>`.
6. The Serial Port menu should display COM2 as the selected. If it does not, choose `Serial Port` and use the arrow keys to change the selection.
7. Set the `Baud Rate` to `19.2K`.
8. Set the `Flow Control` to `CTS/RTS`.
9. Set the `Terminal Type` to `VT-100`.
10. Press `<F10>` to save the configuration changes and exit BIOS Setup.
11. At the prompt to save changes and exit, select `Yes` and press `<Enter>`.
12. This reboots the server with console redirection enabled. Power down the server and configure the console.

Console Configuration
1. Boot the console into the operating system.
2. Launch HyperTerminal by clicking on the `Start` button in the task bar.
3. Select `Programs>Accessories>Communications` and click `HyperTerminal`.
4. At the Connection Description window, enter `guest` for the name and click `OK`.
5. At the Connect To window, select the COM port of the console where the null modem is connected. In this example, it is COM1.
6. At the COM1 Properties window, select `19200` for the Bits per second (Baud rate) to match the SMU configuration on the server.
7. Select `Hardware` for the Flow Control to match the configuration settings for the BIOS Setup (CTS/RTS is the Hardware flow control).
8. Leave the default settings for the other boxes. Click `OK` to accept the settings and enter the HyperTerminal screen.
9. Power on the server. The console starts displaying the redirection once the video synchronizes on the server.

Terminal Mode

The Terminal Mode feature allows you to directly interface to the server's Baseboard Management Controller via a serial port connection and execute text-based commands. Two types of text commands are supported:

- A limited selection of text commands
- Standard binary IPMI 1.5 hex-ASCII commands

Using the terminal mode feature you can do the following:

- Power the server on or off
- Reset the server
- Retrieve the server's health status
- Configure and retrieve the server management subsystems boot options
- Configure and retrieve the BMC's terminal mode configuration
- Execute any platform supported binary command specified in the IPMI v1.5 specification using the hex-ASCII format

See *Terminal Mode Configuration* on page 79 for details about the terminal mode configuration screen.

Setup and Configuration

Connection Mechanism

Two types of connection mechanisms are supported as follows:

- Direct connection, where a local host is connected to the target system directly
- Modem connection, where the local host is connected to the target system via a modem

Hardware Setup

Hardware setup is dependent upon the type of connection mechanism being employed as follows:

- For a direct connection, a null modem cable is needed to connect the local host to the target system
- For a modem connection, the local host and target systems must both be connected to modems via serial cables

Configuration Using System Maintenance Utility (SMU)

Configuration of terminal mode requires proper configuration of the following:

- The serial channel
- User login information (user name and password)
- The terminal mode configuration parameters

The SMU provides methods to access and manipulate all the necessary parameters for terminal mode configuration.

Serial Channel Configuration

The serial channel is configured through the SMU. Set the connection mode to the desired connection mode and the rest of the options to the desired state for your application.

- **Direct Connection Mode:** Set the options on the direct connection mode to the correct states for your application. Disable the ping message to avoid receiving serial ping message data from the BMC on your terminal screen.
- **Modem Connection Mode:** Set the options on the modem connection mode to the desired states for your application. Disable the ping message to avoid receiving serial ping message data from the BMC on your terminal screen.

Save the new serial channel configuration when you are done editing the serial channel settings.

Sample Setup for Terminal Mode

The following is an example of how to configure the console/host and server for Terminal Mode. In this example, the console is running Windows 2000 with SP3. The console and server are directly connected through the serial ports of both systems. See *Serial/Modem Channel Configuration Sub-task* on page 70 for details about the Serial / Modem configuration screens.

Server Configuration

1. Run the SMU to configure the BMC.
2. In the Navigation Pane at the left side of the SMU, click `Serial/Modem` to go to the Serial/Modem configuration menu.
3. At the `Connection Mode` box, pull down the menu and select `Direct Connect Mode`.
4. Select `Always Available` for the `Access Mode`.
5. Select `Administrator` for the `Privilege Level Limit`.
6. Select `None` for `Flow Control`.
7. Leave the `Enable Data Terminal Ready` box unselected.
8. Select `19200` for the `Baud Rate`.
9. Click `Next` to move to the next menu.
10. Click `Next` again to reach the Terminal Mode Configuration screen.
11. Click in the `Enable Terminal Mode` box to select it.
12. Click in the `Enable Line Editing` box to select it.
13. Select `Backspace` for the `Delete Control`.
14. Select the box for `Turn BMC echo of received characters on`.
15. Select the box for `Enable handshake when BMC ready to receive another message` box.
16. Select `CRLF` for the `Newline output sequence (BMC to console)` box.
17. Select `CR` for the `Newline input sequence (console to BMC)` box.
18. Click `Save` to save your settings and click `Ok` to return to the Home page of the SMU.
19. Click on the `User` option in the Navigation Pane to configure the user setup.
20. Select the `Anonymous User` box and click on the `Edit` button to configure this user.
21. In the Edit User Configuration screen, check the `Enable User` box.
22. In the `Enter New Password` box, enter your password. In this example the password is `guest`.
23. Enter the password again in the `Verify New Password` box.
24. Select `Administrator` for the `User Privilege Level` under the Serial/Modem Channel menu.

25. Click `OK` to exit out of this menu. Click `Save` to save the configuration.
26. Click `OK` at the User Save Result menu to return to the Home menu.
27. At the Home menu, click on the `Exit` option in the Navigation pane to exit SMU. Click `OK` to confirm the exit.
28. Reboot the server.

Console Configuration

1. Boot the console into the operating system.
2. Launch HyperTerminal by clicking the `Start` button in the task bar.
3. Select `Programs>Accessories>Communications` and click `HyperTerminal`.
4. At the Connection Description window, enter `guest` for the name and click `OK`.
5. At the Connect To window, select the COM port of the console that the null modem is connected. In this example, it is `COM1`.
6. At the COM1 Properties window, select `19200` for the `Bits per second (Baud rate)` box to the SMU configuration on the server.
7. Select `None` for the `Flow Control` to match the BMC configuration.
8. Leave the default settings for the other boxes. Click `OK` to accept the settings and enter the HyperTerminal screen.
9. The PING message sent by the BMC is displayed as characters on the HyperTerminal screen.
10. Press the `<ESC>` key followed by `<(>` to enable Terminal Mode and end the PING messages. `[TMODE OK]` is displayed.
11. Type `[SYS TMODE]`, it is case sensitive and must be in uppercase. The response is `[OK TMODE]` indicating that Terminal Mode is functioning.

Logging Into the Terminal Mode Session

Reminder: `Guest` was the password set for the Anonymous User in the BMC.

1. At the HyperTerminal screen enter `[SYS PWD -N guest]` to login. `-N` represents the Anonymous User; `guest` is the password. This text is case sensitive.
2. The screen returns `[SYS]` and `[OK]` to indicate a successful login.
3. Type any supported terminal mode command.
4. To logout type `[SYS PWD -X]`

User Configuration

A user must be configured through the SMU to make full use of terminal mode. To create a user, navigate to the SMU user configuration screen. Enter any username and password combinations desired. Make sure to check the box that enables a particular user for use on the serial channel. If this is not done, the username is not useable on the serial channel for terminal mode. Configure the user with the desired maximum privilege level. See *User Configuration Sub-task* on page 60 for details about the user configuration screens.

Spaces, left bracket characters or right bracket characters are not allowed in usernames or passwords used with terminal mode.

Security Information

Terminal mode access to the BMC is governed by the user name and password configuration through the SMU; before the server will accept terminal mode commands, a session must be established. However, a limited selection of text commands and binary hex-ASCII commands that are assigned the lowest IPMI privilege level are available before session establishment with the BMC.

Since the terminal mode password is sent via clear text, the terminal mode session should take place in a secure location over a secure link, preferably via a direct connection. Connection via a modem is supported but not recommended.

Terminal Mode Commands

Input Restrictions

Terminal mode messages are bound by the restrictions listed below.

Switching between Console Redirection and Terminal Mode

When in terminal mode, use the following key sequence to switch to console redirection:

`<ESC><Q>`

When in console redirection, use the following key sequence to switch to terminal mode:

`<ESC><(>`

Syntax

Terminal mode messages follow the general syntax:

`[message data][newline sequence]`

Each terminal mode message must be preceded with the left bracket start character and must be ended with a right bracket stop character and the appropriate input newline sequence.

No input characters are accepted until the start character has been received.

Terminal mode text commands are case sensitive, but hex-ASCII commands can either use upper or lower case letters for ASCII representations of hex digits.

Command Length

Terminal mode messages are limited to a maximum length of a 122 characters. This includes the left and right brackets, but not control characters.

Character Support

Terminal mode messages are allowed to be composed of standard printable ASCII characters. All other characters are treated as illegal characters.

Special Character Handling - <ESC> character

The `<ESC>` character can be used to delete an entire message prior to submission to the BMC for processing. If line editing is enabled, and the `<ESC>` key is followed by an input newline sequence, the BMC responds by outputting an output newline sequence. Otherwise, the BMC goes back to looking for the start character.

Special Character Handling - <DEL> or <BKSP> character

The `<BKSP>` or `<DEL>` key can be used to delete the last character entered if the message has not been submitted to the BMC yet.

Special Character Handling - Line Continuation character

Long IPMI messages can be split across multiple lines by using the line continuation `<\>` character followed immediately by an input newline sequence. Line continuation character usage is supported for both text and hex-ASCII commands.

Special Character Handling - Illegal characters

Any illegal characters received by the BMC clears the message in progress and forces the BMC back to looking for the start character.

Hex-ASCII Command Format

Binary IPMI commands are sent and received as a series of case insensitive hex-ASCII pairs, where each is optionally separated from the preceding pair by a single `<space>` character. The following is an example of a binary IPMI request message:

`[18 00 22]<newline sequence>`

The software ID and LUN for the remote console are fixed and implied by the command. The SWID for messages to the remote console is always 47h, and the Logical Unit Number (LUN) is 00b.

A bridge field is used to identify whether the message should be routed to the BMC's bridged message tracking or not. See the *Terminal Mode IPMI Message Bridging* on page 111 for information.

Table 21.   Terminal Mode Request to BMC

Byte	Explanation
1	[7:2] – Net Function (even) [1:0] – Responder's LUN
2	[7:2] – Requester's Sequence Number [1:0] – Bridge field
3	Command Number
4:N	Data

Table 22.   Terminal Mode Request from BMC

Byte	Explanation
1	[7:2] – Net Function (odd) [1:0] – Responder's LUN
2	[7:2] – Requester's Sequence Number [1:0] – Bridge field
3	Command Number
4	Completion Code
5:N	Data

Text Command Format

Text commands do not support the bridging and sequence number fields present in the hex-ASCII commands, are case sensitive, and are preceded by a prefix consisting of the string SYS.

Examples

Hex-ASCII command example (IPMI Reset Watchdog Cmd):

```
[18 00 22]<CR>
[1C 00 22 00]<CR-LF>
```

Text command example:

```
[SYS TMODE]<CR>
[OK TMODE]<CR-LF>
```

Terminal Mode IPMI Message Bridging

Terminal mode supports the ability to bridge IPMI messages to another interface when binary hex-ASCII IPMI commands are used. The message bridge is determined by the following:

- The bridge field
- Whether the message is a request or a response
- The message direction with respect to the BMC and the LUN.

Table 23 lists the supported BMC combinations for IPMI message bridging. No other combinations are supported. IPMI messages to and from the system interface are transferred using the BMC SMS (System Management Software) LUN, 10b, and with the bridge field set to 00b.

Table 23. Supported BMC Combinations for IPMI Message Bridging

Bridge Field	Request/ Response	Message Direction (to BMC)	LUN	Message Interpretation
00b	Request	In	00b, 01b, 11b	Remote Console request to BMC functionality Message is a request from the remote console to the BMC
00b	Response	Out	00b, 01b, 11b	Response to Remote Console from BMC functionality Message is a response to an earlier request from the remote console to the BMC
00b	Request	In	10b	Remote Console request to SMS Message is a request from the remote console to SMS via the Receive Message Queue
00b	Response	Out	10b	SMS Response to Remote Console Message is a response to an earlier request from SMS
01b	Response	Out	Any	Response to earlier Bridged Request from Remote Console Message is the asynchronous response from an earlier bridged request that was encapsulated in a Send Message command issued to the BMC by the remote console

Table 24.   Terminal Mode Text Commands

Command	Switches	Description
SYS PWD	-U USERNAME `<password>`	Used to activate a terminal mode session. USERNAME corresponds to the ASCII text for the username. `<password>` represents a printable password (up to 16 characters). If `<password>` is not provided, then a null password (all binary 0) is submitted. Passwords are case sensitive. Either the SYS PWD command (or Activate Session IPMI message) must be successfully executed before any command or IPMI messages are accepted. Note that a modem connection may be automatically dropped if multiple bad passwords are entered.
	-N `<password>`	-N represents a Null username. `<password>` represents a printable password (up to 16 characters). If `<password>` is not provided, then a null password (all binary 0) is submitted. Passwords are case sensitive. Either the SYS PWD command (or Activate Session IPMI message) must be successfully executed before any command or IPMI messages are accepted. Note that a modem connection may be automatically dropped if multiple bad passwords are entered.
	-X	-X immediately logs out any presently active session. Entering an invalid password with -U or -N also has the same effect.
SYS TMODE		Used as a no-op confirm that Terminal Mode is active. BMC returns an OK response followed by `TMODE`.
SYS SET BOOT XX YY ZZ AA BB		Sets the boot flags to direct a boot to the specified device following the next IPMI command or action initiated reset or power-on. XX…BB represent five hex-ASCII encoded bytes, which are the boot flags parameter in the Boot Option Parameters. See *Table 25* for information. Upon receiving this command, the BMC automatically sets the valid bit in the boot options and sets all the Boot Initiator Acknowledge data bits to 1b.
SYS SET BOOTOPT XX YY…NN		This is essentially a text version of the IPMI Set System Boot Options command. It allows any of the boot option parameters to be set, not just the boot flags. XX YY…NN represent the hex-ASCII encoding for the data bytes that are passed in the Set System Boot Options request. See *Table 25* for information. XX - Parameter valid [7] - 1b = Mark parameter invalid / locked 0b = Mark parameter valid / unlocked [6:0] - Boot option parameter selector YY…NN -– Boot Option Parameter Data Passing 0-bytes of parameter data allows the parameter valid bit to be changed without affecting the present parameter setting.

Command	Switches	Description
SYS GET BOOTOPT XX YY ZZ		This is essentially a text version of the IPMI "Get System Boot Options" command. It allows any of the boot option parameters to be retrieved.
		XX YY ZZ represents the hex-ASCII for the data bytes that are passed in the Get System Boot Options request.
		The BMC returns the data from the command in hex-ASCII format. See *Table 25* for information.
		XX - Parameter selector
		[7] -Reserved
		[6:0] - Boot option parameter selector
		YY - Set Selector
		[7:0] -Selects a particular block or set of parameters under the given parameter selector
		Write as 00h if parameter does not use a Set Selector
		ZZ - Block Selector
		Selects a particular block within a set of parameters
		Write as 00h if parameter does not use a Block Selector.
		Note: As of this writing, there are no IPMI-specified Boot Options parameters that use the block selector. However, this field is provided for consistency with other configuration commands and as a placeholder for future extension of the IPMI specification.
SYS SET TCFG		Returns the Terminal Mode Configuration bytes where XX and YY represent hex-ASCII encodings for the volatile version of data bytes 1 and 2 as specified in *Table 26*, and AA BB represent hex-ASCII encoding of the non-volatile version.
		V:XX YY<output termination sequence>
		N:AA BB<output termination sequence>
	-V XX YY	This command sets the volatile Terminal Mode Configuration. XX and YY represent hex-ASCII encodings for data bytes 1 and 2 as specified in *Table 26*. The BMC returns the same output as for SYS SET TCFG, above.
	-N XX YY	This command sets the non-volatile Terminal Mode Configuration. XX and YY represent hex-ASCII encodings for data bytes 1 and 2 as specified in *Table 26*. The BMC returns the same output as for SYS SET TCFG, above.
SYS RESET		Directs the BMC to perform an immediate system hard reset.
SYS POWER OFF		Directs the BMC to perform an immediate system power off.
SYS POWER ON		Causes the BMC to initiate an immediate system power on.

Command	Switches	Description
SYS HEALTH QUERY		Causes the BMC to return a high level version of the system health status in terse format. The BMC returns a string with the following format if the command is accepted. PWR:zzz H:xx T:xx V:xx PS:xx C:xx D:xx S:xx O:xx Where: • PWR is system POWER state • H is overall Health • T is Temperature • V is Voltage • PS is Power Supply subsystem • F is cooling subsystem (Fans) • D is hard drive / RAID Subsystem • S is physical Security • O is Other (OEM) zzz is: ON, OFF (soft-off or mechanical off), SLP (sleep - used when it cannot distinguish sleep level), S4, S3, S2, S1, ?? (unknown) xx is: ok, nc, cr, nr, uf, or ?? where: • ok = OK (monitored parameters within normal operating ranges) • nc = non-critical (warning: hardware outside normal operating range) • cr = critical (fatal: hardware exceeding specified ratings) • nr = non-recoverable (potential damage: system hardware in jeopardy or damaged) • uf = unspecified fault (fault detected, but severity unspecified) • ?? = status not available/unknown (typically because system power is OFF)
	-V	Causes the BMC to return a high level version of the system health status in multi-line verbose format. The BMC returns a string of the following format: SYS Health:xx<output termination sequence> Power: ON, OFF (soft-off or mechanical off), SLEEP (sleep - used when it cannot distinguish sleep level), S4, S3, S2, S1, Unknown Temperature:xx<output termination sequence> Voltage:xx<output termination sequence> PowerSystem:xx<output termination sequence> Cooling:xx<output termination sequence> Drives:xx<output termination sequence> Security:xx<output termination sequence> Other:xx<output termination sequence> Where xx is: • OK: monitored parameters within normal operating ranges • Non-critical: warning: hardware outside normal operating range • Critical: fatal hardware exceeding specified ratings • Non-recoverable: potential damage: system hardware in jeopardy or damaged • Unspecified fault: fault detected, but severity unspecified • Unknown: status not available/unknown (typically because system power is OFF)

Table 25.   Boot Option Parameters

Parameter	#	Parameter Data (non-volatile unless otherwise noted)
Set In Progress (volatile)	0	Data 1 - This parameter is used to indicate when any of the following parameters are being updated, and when the updates are completed. The bit is primarily provided to alert software that some other software or utility is in the process of making changes to the data. The change shall take effect when the write occurs.
		[7:2] - Reserved
		[1:0] - 00b = Set complete. If a system reset or transition to powered down state occurs while Set in Progress is active, the BMC goes to the Set Complete state. If rollback is implemented, going directly to Set Complete without doing a Commit Write causes pending write data to be discarded.
		01b = Set in progress. This flag indicates that some utility or other software is presently doing writes to parameter data. It is a notification flag only, it is not a resource lock. The BMC does not provide any interlock mechanism that would prevent other software from writing parameter data while.
		10b = Reserved
		11b = Reserved
Service partition selector (semi-volatile)[1]	1	Data 1
		[7:0] - Service partition selector. This value is used to select the service partition BIOS should boot using. This document does not specify which value corresponds to a particular service partition.
		00h = Unspecified
Service partition scan (semi-volatile)[1]	2	Data 1
		[7:2] - Reserved
		[1] - 1b = Request BIOS to scan for specified service partition. The BIOS clears this bit after the requested scan has been performed.
		[0] - 1b = Service Partition discovered. The BIOS sets this bit to indicate it has discovered the specified service partition. The BIOS must clear this bit on all system resets and power ups, except when a scan is requested.
BMC boot flag valid bit clearing (semi-volatile)[1]	3	Data 1 - BMC boot flag valid bit clearing. Default = 0000b.
		[7:5] - Reserved
		[4] - 1b = Do not clear valid bit on reset/power cycle caused by PEF
		[3] - 1b = Do not automatically clear boot flag valid bit if IPMI Chassis Control command not received within 60-second timeout (countdown restarts when a IPMI Chassis Control command is received)
		[2] - 1b = Do not clear valid bit on reset/power cycle caused by watchdog timeout
		[1] - 1b = Do not clear valid bit on push-button reset / soft-reset (e.g. <Ctrl><Alt><Del>)
		[0] - 1b = Do not clear valid bit on power up via power push-button or wake event

Parameter	#	Parameter Data (non-volatile unless otherwise noted)
Boot info acknowledge (semi-volatile)[1]	4	These flags are used to allow individual parties to track whether they have seen and handled the boot information. Applications that deal with boot information should check the boot info and clear their corresponding bit after consuming the boot options data.
		Data 1: Write Mask (Write-only: This field is returned as 00h when read. This is to eliminate the need for the BMC to provide storage for the Write Mask field.)
		[7] - 1b = enable write to bit 7 of Data field
		[6] - 1b = enable write to bit 6 of Data field
		[5] - 1b = enable write to bit 5 of Data field
		[4] - 1b = enable write to bit 4 of Data field
		[3] - 1b = enable write to bit 3 of Data field
		[2] - 1b = enable write to bit 2 of Data field
		[1] - 1b = enable write to bit 1 of Data field
		[0] - 1b = enable write to bit 0 of Data field
		Data 2: Boot Initiator Acknowledge Data
		The boot initiator should typically write FFh to this parameter prior to initiating the boot. The boot initiator may write 0s if it wants to intentionally direct a given party to ignore the boot info. This field is automatically initialized to 00h when the management controller is first powered up or reset.
		[7] - reserved. Write as 1b. Ignore on read
		[6] - reserved. Write as 1b. Ignore on read
		[5] - reserved. Write as 1b. Ignore on read
		[4] - 0b = OEM has handled boot info
		[3] - 0b = SMS has handled boot info
		[2] - 0b = OS / service partition has handled boot info
		[1] - 0b = OS Loader has handled boot info
		[0] - 0b = BIOS/POST has handled boot info

Parameter	#	Parameter Data (non-volatile unless otherwise noted)

Boot flags (semi-volatile)[1]	5	**Data 1**
		
		[7] - 1b = Boot flags valid. The bit should be set to indicate that valid flag data is present. This bit may be automatically cleared based on the boot flag valid bit clearing parameter, above
		
		[6:0] - Reserved
		
		BIOS support for the following flags is optional. If a given flag is supported, it must cause the specified function to occur in order for the implementation to be considered to be conformant with this specification.
		
		The following parameters represent temporary overrides of the BIOS default settings. BIOS should only use these parameters for the single boot where these flags were set. If the bit is 0b, BIOS should use its default configuration for the given option.
		
		Data 2
		
		[7] - 1b = CMOS clear
		
		[6] - 1b = Lock Keyboard
		
		[5:2] - Boot device selector
		    0000b = No override
		    0001b = Force PXE
		    0010b = Force boot from default Hard-drive[2]
		    0011b = Force boot from default Hard-drive, request Safe Mode[2]
		    0100b = Force boot from default Diagnostic Partition[2]
		    0101b = Force boot from default CD/DVD[2]
		    0110b-1110b = Reserved
		    1111b = Force boot from Floppy/primary removable media
		
		[1] - 1b = Screen Blank
		
		[0] - 1b = Lock out reset buttons

Boot flags (semi-volatile)[1] (continued)	5	**Data 3**
		
		[7] - 1b = Lock out (power off/ sleep request) via power button
		
		[6:5] - Firmware (BIOS) Verbosity (Directs what appears on POST display)
		    00b = System default
		    01b = Request quiet display
		    10b = Request verbose display
		    11b = reserved
		
		[4] - 1b = Force progress event traps. When set to 1b, the BMC transmits PET traps for BIOS progress events to the LAN or serial/modem destination for the session that set the flag. Since this capability uses PET traps, this bit is ignored if for connection modes that do not support PET such as Basic Mode and Terminal Mode
		
		[3] - 1b = User password bypass. When set to 1b, the managed client's BIOS boots the system and bypasses any user or boot password that might be set in the system
		
		[2] - 1b = Lock sleep button. When set to 1b, directs BIOS to disable the sleep button operation for the system, normally until the next boot cycle
		
		[1:0] -00b = Console redirection occurs per BIOS configuration setting
		    01b = Suppress (skip) console redirection if enabled
		    10b = Request console redirection be enabled
		    11b = Reserved

Parameter	#	Parameter Data (non-volatile unless otherwise noted)
Boot flags (semi-volatile)[1] (continued)	5	Data 4 [7:4] - Reserved [3] - BIOS Shared Mode Override Can be used to request BIOS to temporarily place the channel into Shared access mode. Per the recommendations in the IPMI specification, Shared access would cause the baseboard serial controller to both remain enabled after POST/start of OS boot, while also allowing the BMC to be accessible. This can be useful when booting to an alternative device such as a Diagnostic Partition since it means the partition can use the serial port but that communication with the BMC can remain available if the partition software fails. 1b = Request BIOS to temporarily set the access mode for the channel specified in parameter #6 to Shared. This is typically accomplished by sending a Set Channel Access command to set the *volatile* access mode setting in the BMC 0b = No request to BIOS to change present access mode setting [2:0] - BIOS Mux Control Override Can be used to request BIOS to force a particular setting of the serial/modem mux at the conclusion of POST / start of OS boot. This override takes precedence over the mux settings for the access mode even if the BIOS Shared Mode Override is set. 000b = BIOS uses recommended setting of the mux at the end of POST. 001b = Requests BIOS to force mux to *BMC* at conclusion of POST/start of OS boot. If honored, this overrides the recommended setting of the mux at the end of POST. 010b = Requests BIOS to force mux to *system* at conclusion of POST/start of OS-boot. If honored, this overrides the recommended setting of the mux at the end of POST. Data 5 - Reserved
Boot initiator info (semi-volatile)[1]	6	Address & Identity information for the party that initiated the boot. The party that initiates the boot writes this parameter and the boot info acknowledge parameter prior to issuing the command that causes the system power up, power cycle, or reset. This data is written by the remote console application, not the BMC. Boot Source Data 1- Channel Number. Channel that delivers the boot command (e.g. chassis control). BIOS and boot software (e.g. service partition or OS loader) can use the *Get Channel Sessions* to find out information about the party that initiated the boot [7:4] - Reserved [3:0] - Channel Number Data 2:5 - Session ID. Session ID for session that the boot command will be issued over. This value can be used with the *Get Channel Sessions* command to find out information about the party that initiated the boot Data 6:9 - Boot Info Timestamp. This timestamp is used to help software determine whether the boot information is stale. A service partition or OS loader may elect to ignore the boot information if it is older than expected The boot initiator should load this field with the timestamp value from the IPMI Get SEL Time command prior to issuing the command that initiates the boot.

Parameter	#	Parameter Data (non-volatile unless otherwise noted)
Boot initiator mailbox (semi-volatile)[1][2]	7	This parameter is used as a mailbox for holding information that directs the operation of the OS loader or service partition software.
		Note: Since this information is retained by the BMC and may be readable by other software entities, care should be taken to avoid using it to carry secret data.
		Data1: Set Selector = Block selector
		Selects which 16-byte info block to access. 0-based.
		Data 2: (17) Block data
		The first three bytes of block #0 are required to be an IANA Enterprise ID Number (least significant byte first) for the company or organization that has specified the loader.
		Up to 16-bytes per block of information regarding boot initiator, based on protocol and medium.
		The BMC supports five blocks of storage for this command. Previous values are overwritten. The BMC does not automatically clear any remaining data bytes if fewer than 16 bytes are written to a given block.
All other parameters	All Others	Reserved

1. The designation 'semi-volatile' means that the parameter will be kept across system power cycles, resets, system power on/off, and sleep state changes, but is not preserved if the management controller loses standby power or is cold reset. Parameters designated as semi-volatile are initialized to 0s upon controller power up or hard reset, unless otherwise specified.

5. IPMI allows software to use the boot initiator mailbox as a way for a remote application to pass OEM parameters for additional selection of the boot process and direction of the startup of post-boot software. If additional parameters are not included, the system boots the primary/first-scanned device of the type specified.

Table 26. Terminal Mode Configuration

Byte	Explanation
1	[7:6] - Reserved
	[5] - Line Editing
	0b = Disable
	1b = Enable (Factory default)
	[4] - Reserved
	[3:2] - Delete control (only applies when line editing is enabled)
	00b = BMC outputs a <DEL> character when <BKSP> or < DEL > is received
	01b = BMC outputs a < BKSP >< SP >< BKSP > sequence when < BKSP > or < DEL > is received (Factory default)
	[1] - Echo control0b = No echo 1b = Echo (BMC echoes characters it receives) (Factory default)
	[0] - Handshaking - BMC outputs a [SYS]<newline> after receiving each terminal mode IPMI message and is ready to accept the next message
	0b = Disable
	1b = Enable (Factory default)

2	[7:4] -	Output newline sequence (BMC to console). Selects what characters the BMC uses as the <newline> sequence when the BMC writes a line to the console in Terminal Mode
		0h = no termination sequence
		1h = <CR-LF> (Factory default)
		2h = <NULL>
		3h = <CR>
		4h = <LF-CR>
		5h = <LF>
		All other = reserved
	[3:0] -	Input newline sequence (Console to BMC). Selects what characters the console uses as the <newline> sequence when writing to the BMC in Terminal Mode
		0h = reserved
		1h = <CR> (Factory default)
		2h = <NULL>
		All other = reserved

Shutting Down the Server

To shut down the server you must exit the operating system (if applicable) and then use the power button to power down the server.

Follow these steps to power down the server.

1. If the server is running an operating system, use the operating system commands or GUI to logoff if necessary and exit the operating system. Successfully exiting the operating system causes the following prompt to appear:
   `Shell>`

2. When this prompt appears, press and hold the power button for several seconds to power down the server.

⚠ **CAUTION**

Powering down the server with the power button does not remove all power from the system. The +5 V standby power is still available to the system even when it has been powered down. To remove standby power from the system you must unplug both power cords from the chassis.

Servicing the System (basic knowledge)

A Warning and Cautions

Before Top Cover or Module Removal

Before removing the top cover or system modules, follow all safety guidelines given below.

1. Turn off all peripheral devices connected to the system.
2. Power down the system by pressing and holding the power button on the front of the chassis for several seconds.
3. After the server shuts down, unplug both AC power cords to remove standby power from the server.

4. Provide electrostatic discharge (ESD) protection by wearing an antistatic wrist strap attached to chassis ground of the system—any unpainted metal surface—when handling components.

⚠ **CAUTION**

> The NovaScale 4020 Server exceeds the 240 VA energy hazard limits that define an operator-accessible area. As a result, only qualified technical individuals should access the processor, memory, and non-hot-swap areas while the system is energized.

📝 **NOTE**

> When replacing hot-swap components, it is not necessary to turn off all peripheral devices, power down the server, or unplug the AC power cords. It **is** necessary to provide ESD protection. See the instructions for the specific hot-swap component for any other safety guidelines.

B Working Inside the System

Handling the Black Cover on Desktop Models

On desktop models the server is equipped with a black cover. Figure 50 shows the black cover removed.
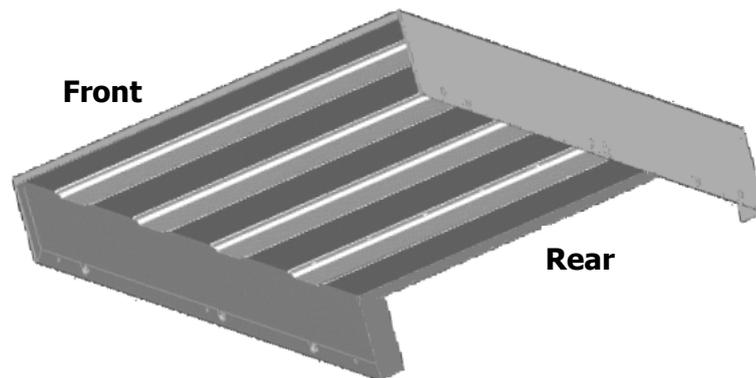
Figure 50. NovaScale 4020 Desktop Black Cover

Before accessing inside the server, for example to add PCI boards, this black cover must be removed.

Removing the Black Cover

To remove the black cover, follow these instructions:
1. Remove the front bezel from the server
2. Using a screwdriver, remove the 6 screws located on the sides of the black cover (3 on each side).
3. Push the black cover back towards the back of the system, approximately 1 centimetre towards the rear.
4. Lift the black cover, first at the rear, then at the front; and remove it.

⚠ **CAUTION**

The black cover is somewhat heavy (8 kgs)

Installing the Black Cover

To install the black cover on the server chassis, follow these instructions:

1. Hold the black cover at the front and at the rear and position it above the chassis of the server.

⚠ **CAUTION**

The black cover is somewhat heavy (8 kgs)

2. Carefully lower the black cover, first at the front, in order that both sides of the black cover position against the J-rails (see Figure 51) located on each side of the server.

Figure 51. J-rails

The front of the black cover must be about 1 centimetre back from the front of the server in order that the 6 pins on the sides of the black cover insert inside the corresponding notches located on the J-rails

3. After the front of the black cover is fully lowered, lower the rear of the black cover, finishing by snapping it.
4. Slide the black cover forward by about 1 centimetre until the front of the black cover aligns the front of the server
5. Install the 6 screws on the sides of the black cover and tighten them.
6. Put in place the front bezel.

Identifying Chassis Modules

The figure below shows the chassis with the top cover removed. Several component areas can be identified, including the processor air duct, memory area (eight DIMM sites, obscured), The PCI riser assembly, the electronics bay (E-Bay), and the peripheral bay. In addition, the chassis supports three hot-swap power supplies, six fans, three PCI cards, one ATA DVD / CD-ROM drive, and two SCSI (SCA-2) hard drives.
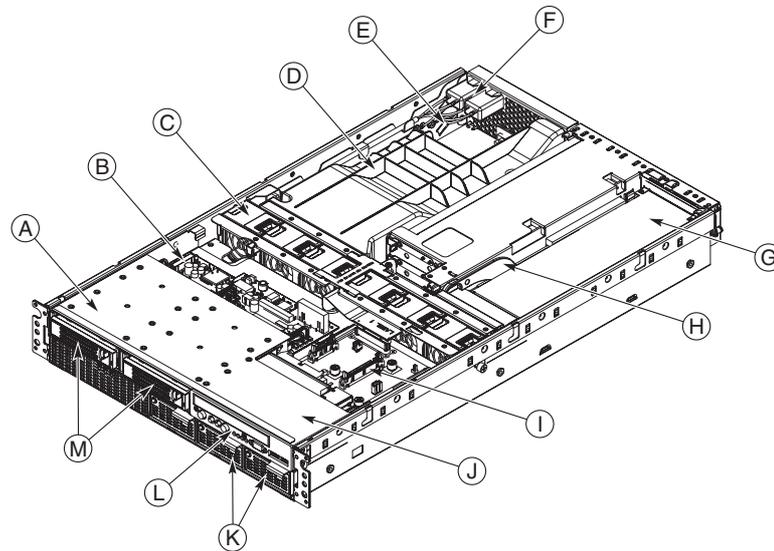
TP00312

A. Peripheral bay	B. SCSI backplane
C. Fan bay	D. Processor air duct (processor(s) installed underneath)
E. Electronics bay	F. Dual AC
G. DIMM sockets (underneath installed PCI card)	H. PCI riser assembly
I. Front panel board	J. Power bay
K. Hot swap power modules	L. Front panel
M. Hot swap hard disk drives	N.

Figure 52. Locating System Modules

Removing and Installing the Top Cover

⚠ **WARNING**

> **Make sure that the rack is anchored securely so it will not tilt forward when the server chassis is extended. A crush hazard exists should the rack tilt forward.**

⚠ **CAUTION**

> Do not leave the chassis cover open or a system fan removed any longer than necessary; system cooling could be reduced. Do not operate the server with the cover removed.

Removing the Top Cover

To remove the top cover, refer to *Figure 53* and follow these instructions:

1. Observe the safety and ESD precautions described in *Warnings and Cautions* and in *Before Top Cover or Module Removal* on page 121.
2. If the chassis is rack-mounted, slide the chassis out far enough to expose the back area of the top cover (see cautions and warnings above).
3. To open the top cover, use a screwdriver or a coin to turn the locking mechanism to the unlocked position.
4. Push the top cover towards the back of the system until it stops, approximately 1-inch towards the rear.
5. Lift the cover up from the front and remove it from the chassis.
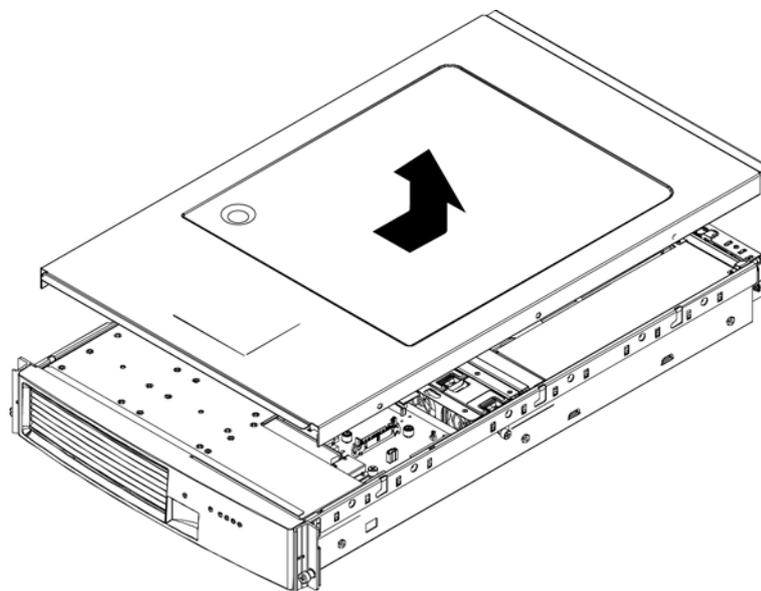
Figure 53. Removing the Top Cover

Installing the Top Cover

To install the top cover, refer to *Figure 54* and follow these instructions:

1. Carefully lower the top cover onto the chassis, inserting the interlock studs in the top cover into the corresponding slots in the chassis.

2. Slide the top cover forward until it engages underneath the front lip of the chassis and stops snug with the forward lip of the peripheral bay.

3. Use a screwdriver or a coin to turn the locking mechanism to the locked position to secure the cover.
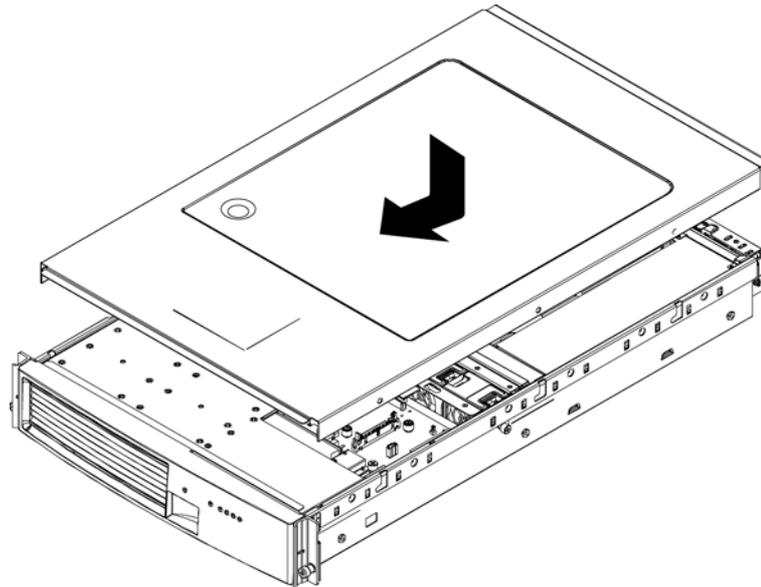
Figure 54. Installing the Top Cover

C Hot-swapping System Components

Hot-swap Hard Drives

The procedures in this section describe how to determine drive status, remove a faulty drive, and install a new drive. For more information, see *Hot-swap Hard Drive Carrier* on page 6.

Determining Drive Status

The carriers contain light-pipes that allow light from dual-color LED indicators on the SCSI backplane board to travel across the carrier and show through the bezel to display hard drive status. The status indicators are described in the table below.

Table 27. SCSI Drive Status LED Descriptions

Feature	Description
Green, flashing	Indicates the hard drive is active
Yellow/Green flashing	Indicates a hard drive fault and hard drive is powered
Yellow/Blank flashing	Indicates a hard drive fault and hard drive is not powered
Not illuminated	Indicates nothing is installed in the bay

Removing a Hard Drive Carrier

1. When replacing a failed drive, examine the amber LEDs to determine which drive has failed. See letter "A" in *Figure 55*. See *Table 27* for information on how to interpret the LEDs.
2. Pull the drive carrier latch open and use the handle to pull the drive assembly toward you. See letter "C" in the figure.
3. Slide the assembly from the bay and place it on a clean, static-free work surface. See letter "D" in the figure below.
4. To mount a new hard drive into the carrier, continue with *Mounting a Hard Drive into a Carrier* on page 130.
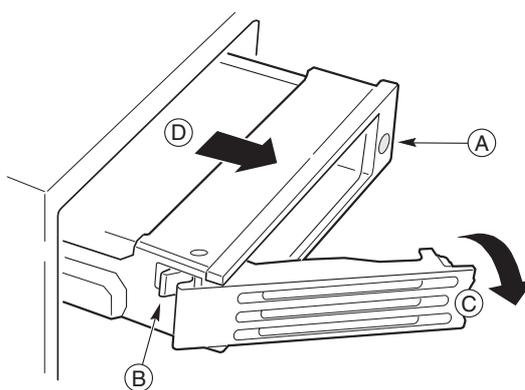
TP00315

A. Hard drive LED	B. Release tab
C. Carrier latch	D. Slide assembly from bay

Figure 55. Removing a Hard Drive Carrier

Mounting a Hard Drive into a Carrier

The server system supports two hot-swap drive carriers in the peripheral bay. Each carrier houses a standard one-inch high SCSI-2 or SCSI-3 hard drive.

⚠ **CAUTION**

> To allow proper airflow and server cooling, all drive bays must contain either a carrier with a hard drive installed or a carrier with an air baffle installed.

To mount a hard drive in a carrier:

1. Remove the hard drive from the protective wrapper and place it on a clean ESD-protected work surface.
2. Record the model and serial number of the drive in your equipment log
3. Set any jumpers and/or switches on the drive according to the drive manufacturer's instructions.
4. If the drive carrier is installed in the drive bay, remove it and place it on a clean static-free work surface. See *Removing a Hard Drive Carrier* above for instructions.
5. If you are installing a hard drive into a carrier that did not previously have a drive installed into it, remove the air baffle. The air baffle is removed by removing the four mounting screws from the drive rails. See letter "A" in *Figure 56*. Store the air baffle for future reinstallation in the event you operate your server without a drive in one of the bays.
6. If you are removing a failed hard drive, remove the four mounting screws that hold the drive into the carrier.
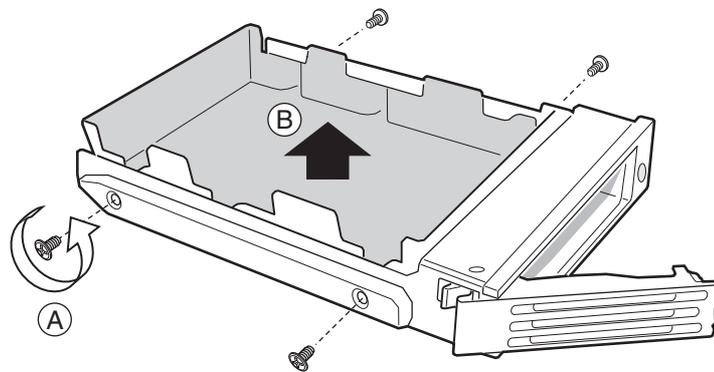
TP00316

A. Screws
B. Lift air baffle

Figure 56. Removing Air Baffle from Hard Drive Carrier

7. Position the carrier as shown *Figure 57*.
8. Place the drive in the carrier with the drive label-side up and the SCA (80 Pin) SCSI connector end of the drive facing the back of the carrier. See letter "A" in the figure.
9. Align the holes in the drive to the holes in the drive carrier and drive rails. Insert the mounting screws that were removed in the previous steps to and secure the carrier to the drive. See letter "C" in the figure below.
10. Continue with the instructions under *Installing a Hard Drive Carrier*.
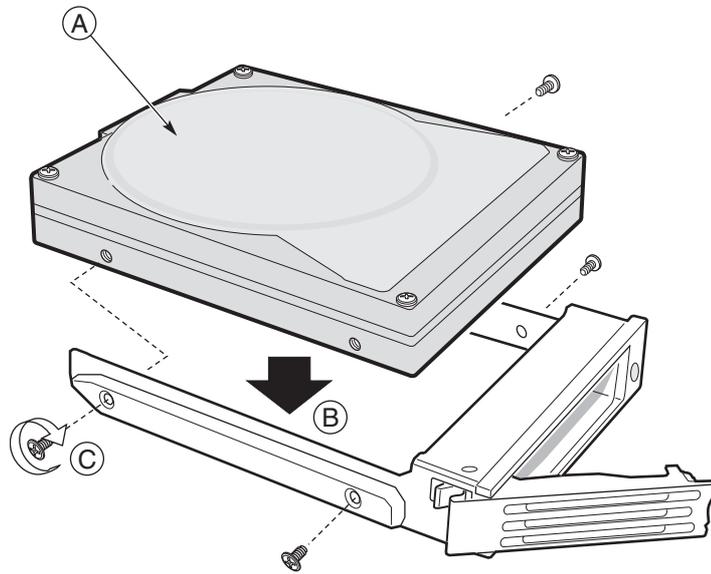
TP00317

A. Hard drive
B. Lower drive into carrier
C. Screws

Figure 57. Attaching the Hard Drive to the Carrier

Installing a Hard Drive Carrier

1. With the drive carrier handle open fully, place the drive carrier into the peripheral drive bay. See letter "A" in *Figure 58*.
2. Slide the drive carrier all the way into the drive bay.
3. Using the drive carrier handle, firmly push the assembly into the bay until the drive docks with the SCSI backplane connector.
4. Swing the drive carrier handle closed until it latches. See letter "B" in the figure below.
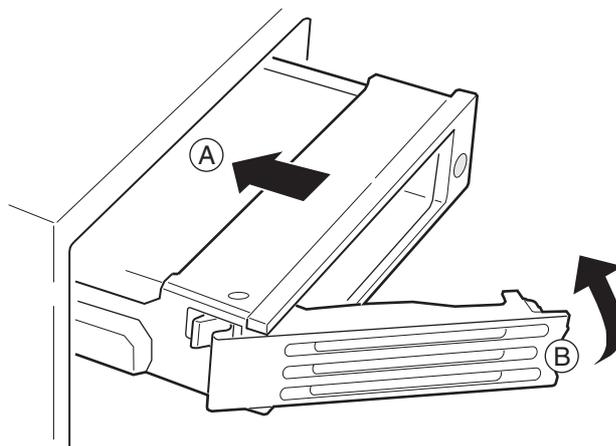
TP00315A

A. Slide drive carrier into chassis
B. Carrier handle

Figure 58. Inserting a Hard Drive

Hot-swap System Fans

The six (60x60x38 mm) cooling fans provide 50CFM of airflow each. The server system supports only a fully populated system fan configuration. However, the server system will continue to meet the thermal specifications if a fan fails. The six fans are mounted side-by-side in the fan bay across the center section of the chassis. The fans can be hot-swapped; they can be removed and re-installed without turning the server system power off.

The procedures in this section describe how to identify a failed fan and replace a failed fan. See *Cooling Subsystem* on page 13 for more information about the operation of the system fans.

Determining Fan Failure

Each fan uses an amber LED to indicate the failed fan. The LED for each fan illuminates only when a fan fails. When an LED illuminates the associated fan should be replaced. To view the LEDs:

1. See the warnings and cautions under *Removing and Installing the Top Cover* on page 126.
2. Follow the instructions under *Removing the Top Cover*.
3. Locate the fan bay. See *Figure 52* for location information.
4. If a fan has failed, the LED for that fan will display an amber LED. See letter "A" in *Figure 59* for help in locating the LEDs.
5. To replace a failed fan, see *Replacing a System Fan*. If no fan has failed, follow the instructions under *Installing the Top Cover*.

Replacing a System Fan

Refer to *Figure 59* and use the instructions below to replace a hot-swap system fan:

1. See the warnings and cautions under *Removing and Installing the Top Cover* on page 126.
2. Follow the instructions under *Removing the Top Cover*.
3. Follow the instructions under *Determining Fan Failure* to identify the failed fan.
4. Place your fingers into the fan access points and squeeze your fingers together to release the fan latch and remove the fan. See letter "B" *Figure 59*.
5. Insert the replacement fan into place. It will fit only one way into the opening and will easily click into place.
6. Follow the instructions under *Installing the Top Cover*.
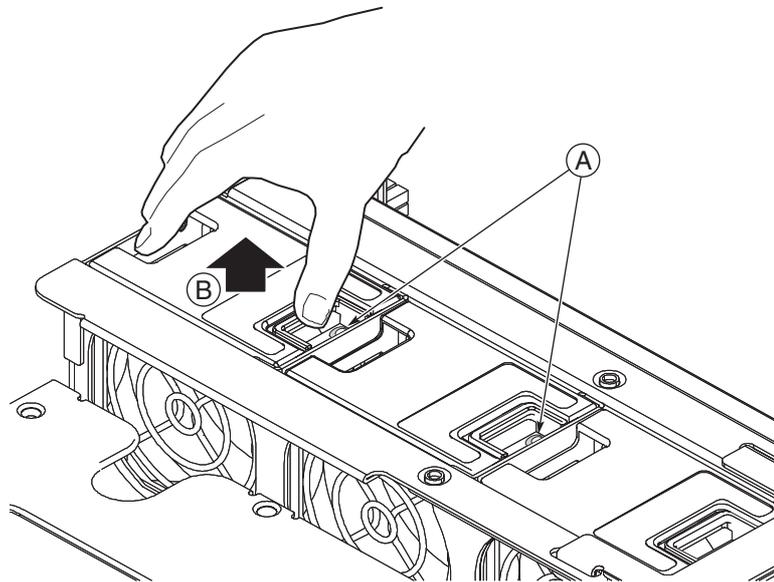
TP00318

A. Fan LEDs (two of six pointed out)
B. Access points

Figure 59. System Fan Location and Removal

Hot-swap Power Supplies

The power subsystem contains the power bay. The power bay includes the AC transfer switch, the power distribution logic, and locations for the three hot-swappable Thin Power Supply modules (TPS). TPS positions are labled AC1/PS1, AC2/PS2, and PS Shared. The power system is rated at 650-watts; the requirements of a fully-loaded system require that at least two operational TPS modules (350-watts each) be installed at any one time. A fully redundant power configuration requires three modules be installed, with the third module (PS Shared) acting as standby module in case one of the first two modules fails.

When a failure occurs, the AC transfer switch will immediately fail-over to the standby TPS module in the PS-shared position. The failing TPS module can be removed and replaced without powering down the server. After replacing the failed TPS module, the AC transfer switch will engage the replaced module and set the module in the PS-Shared position back to standby.

See *Power Supply Bay* on page 8 and *Power Subsystem* on page 16 for more information.

NOTES

> A system operating in a two TPS configuration should have a TPS filler panel installed in the PS-Shared position to optimize cooling. Server systems that are shipped with with two TPSs have a filler panel installed at the factory.

Determining Power Supply Status

Each TPS module has a bi-color LED at the top left corner of the module that indicates the status and health of the module. *Table 28* provides more detail on the LEDs.

Table 28.   Power Supply LEDs

Power Supply Condition	Power Supply LED
No AC power to any PSU	Off
No AC power to this PSU only	Amber
AC present / Only standby outputs on	Blink green
Power supply DC outputs on and ok	Green
Power supply failure (includes over voltage and over temperature)	Amber
Current limit	Amber

Power Module Removal and Replacement

⚠ CAUTION

If your server system is operating in a non-redundant power supply configuration (without a power supply in the PS-Shared location), you need to power down your server system before replacing a failed power supply. Failure to do so will cause an immediate and uncontrolled power down.

Refer to *Figure 60* and use the following instructions to replace a power supply:

1. Locate the power module to be removed. Look at the LED at the top left corner of each module and refer to *Table 28* to determine the status of the modules.
2. Squeeze the thumb latch to unlock the power supply handle and pull the handle to undock the power supply. See letter "A" in Figure 60.
3. Pull the power supply out of the chassis and set it aside. See letter "B" in the figure below.
4. Align the replacement TPS module in the power bay, slide back until latched.
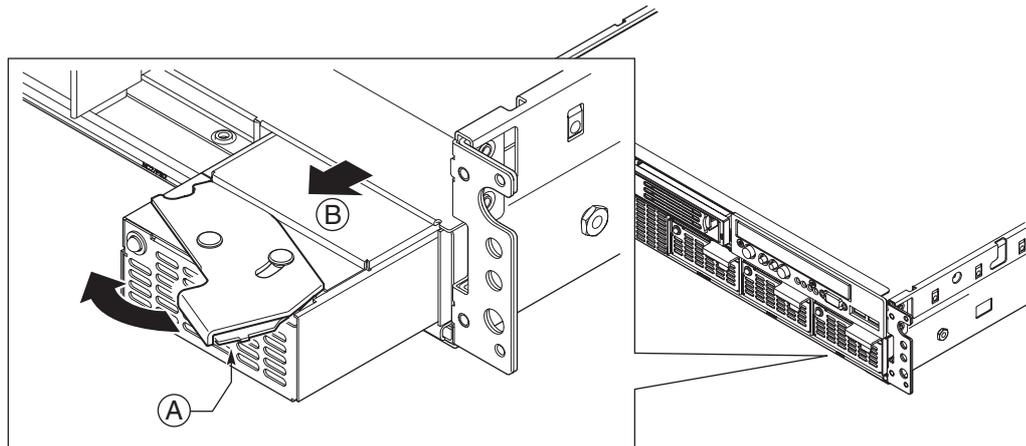
TP00319

A. Latch
B. Pull module from chassis

Figure 60. Removing and Replacing Power Module

D Servicing the Electronics Bay

Adding or Replacing PCI Cards

⚠ **CAUTION**

Remove the AC power cords from the system. Damage to the system can occur if AC power is not disconnected from the system prior to removal or installation of the PCI riser assembly.

The PCI riser assembly contains the following active components:

- One server I/O Hub (SIOH) component of the E8870 chip set
- One P64H2 PCI-X bridge component
- Three non-hot-plug able PCI-X slots
  - One 64-bit, 133 MHz PCI-X, full length
  - Two 64-bit, 100 MHz PCI-X, full length
- An integrated DC-to-DC voltage converter
- Server management logic
- I^2C logic
  - Field Replaceable Unit (FRU) device ID ROM
  - Temperature sensor

The PCI riser assembly needs to be removed from the chassis in order to add or remove PCI cards. Refer to the following instructions.

Removing the PCI Riser Assembly

To remove the PCI riser assembly from the chassis, refer to *Figure 61* and follow these instructions:

1. See the warnings and cautions under *Removing and Installing the Top Cover* on page 126 .
2. Turn off all peripheral devices connected to the system.
3. Power down the system by pressing and holding the power button on the front panel for several seconds. Unplug both AC power cords to remove standby power from the server.
4. Follow the instructions under *Removing the Top Cover*.
5. Disconnect all peripheral cables attached to adapters that are installed in the PCI riser assembly.
6. Firmly grasp the riser release mechanism lever and slowly pull up and back on the lever. Some force may be required. See letter "A" in *Figure 61*. The riser assembly will disengage from the main board.
7. Lift the riser assembly straight up to remove it from the chassis. See letter "B" in the figure.

⚠ **CAUTION**

When removing the riser assembly, do not attempt to remove it at an angle. Removal at any other orientation other than vertical could result in damage to the VHDM connectors.
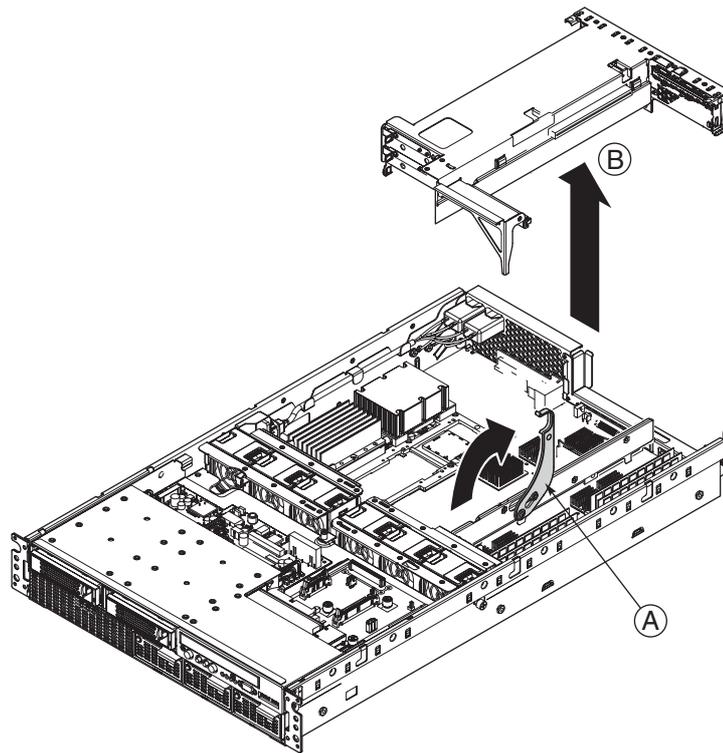
TP00320

A. Handle
B. Lift assembly straight up

Figure 61. Removing PCI Riser Assembly

Installing PCI Cards

1. With the PCI riser assembly removed, locate the slot into which the card is to be installed. See the table below for information about the slots.
2. Open the lever over the shields (see letter "A" in *Figure 62)* to remove the shield (see letter "B" in *Figure 62)*.
3. Press down on the touch point on the PCI retention lever for the slot and swing the lever open. See letter "C" in *Figure 62*.
4. Insert the adapter card and apply sufficient pressure to set the card into the slot. See letter "D" in *Figure 62*.
5. Move the touch point and shield levers to the closed positions and snap to secure them.
6. Repeat steps 1 – 5 for each card to be installed.

Slot	Connector	PCI Bus	Key	Speed	Form Factor
Slot 1	J9L1 (Pin Side)	Bus B	3.3 V	100 MHz PCI-x	Long
Slot 2	J1A1 (Top Component Side)	Bus B	3.3 V	100 MHz PCI-x	Long
Slot 3	J1A3 (Bottom Component Side)	Bus A	3.3 V	133 MHz PCI-x	Long
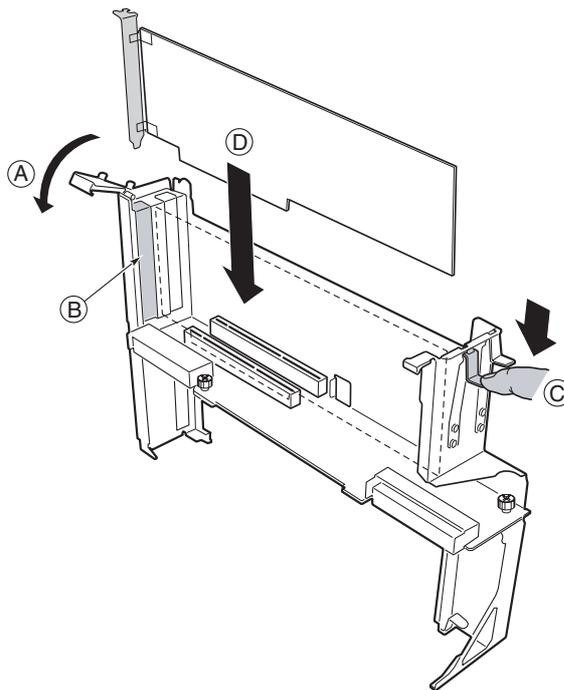
A. Shield latch   B. Shield
C. Touch point   D. Insert card

Figure 62. Inserting a PCI Card

Installing the PCI Riser Assembly

⚠ CAUTION

When inserting the riser assembly, do not attempt to insert it at an angle.
Insertion at any other orientation other than vertical could result in
damage to the VHDM connectors.

1. Align the PCI riser card assembly with its mating slot on the retention lever assembly.
2. Lower the PCI riser assembly into position.
3. Move the PCI riser retention lever forward and down to engage the VHDM connectors and seat the PCI riser assembly firmly into position.
4. Connect any peripheral cables that attached to PCI adapters installed in the riser assembly. See the documentation that came with your PCI adapter for information.
5. Follow the instructions under *Installing the Top Cover* on page 127.
6. Reconnect any peripheral devices previously disconnected.

Replacing the Battery

The lithium battery on the main board powers the real-time clock (RTC) for three to four years in the absence of power. When the battery weakens, the loss of voltage will cause the system settings and selections stored in CMOS RAM and Real Time Clock (such as the date and time) to loose their preselected values. Contact your customer service representative or dealer for a list of approved replacement batteries.

The following warning and translations are required by specific certifying agencies to be printed immediately adjacent to the procedure for removing the battery.

⚠ **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.

Safety Warnings

WARNING: English (US)

AVERTISSEMENT: Français

WARNUNG: Deutsch

AVVERTENZA: Italiano

ADVERTENCIAS: Español

NovaScale 4020 User's Guide

WARNING: English (US)
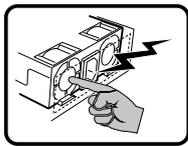
The power supply in this product contains no user-serviceable parts. There may be more than one supply in this product. Refer servicing only to qualified personnel.
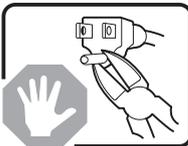
Do not attempt to modify or use the supplied AC power cord if it is not the exact type required. A product with more than one power supply will have a separate AC power cord for each supply.
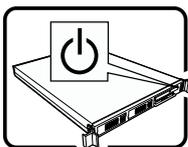
The power button on the system does not turn off system AC power. To remove AC power from the system, you must unplug each AC power cord from the wall outlet or power supply.

The power cord(s) is considered the disconnect device to the main (AC) power. The socket outlet that the system plugs into shall be installed near the equipment and shall be easily accessible.

SAFETY STEPS: Whenever you remove the chassis covers to access the inside of the system, follow these steps:

1. Turn off all peripheral devices connected to the system.
2. Turn off the system by pressing the power button.
3. Unplug all AC power cords from the system or from wall outlets.
4. Label and disconnect all cables connected to I/O connectors or ports on the back of the system.
5. Provide some electrostatic discharge (ESD) protection by wearing an antistatic wrist strap attached to chassis ground of the system—any unpainted metal surface—when handling components.
6. Do not operate the system with the chassis covers removed.
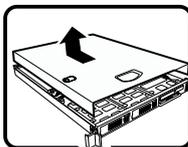
After you have completed the six SAFETY steps above, you can remove the system covers. To do this:

1. Unlock and remove the padlock from the back of the system if a padlock has been installed.
2. Remove and save all screws from the covers.
3. Remove the covers.
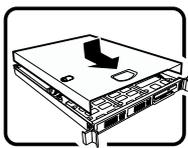
For proper cooling and airflow, always reinstall the chassis covers before turning on the system. Operating the system without the covers in place can damage system parts. To install the covers:

1. Check first to make sure you have not left loose tools or parts inside the system.
2. Check that cables, add-in boards, and other components are properly installed.
3. Attach the covers to the chassis with the screws removed earlier, and tighten them firmly.
4. Insert and lock the padlock to the system to prevent unauthorized access inside the system.
5. Connect all external cables and the AC power cord(s) to the system.
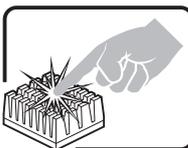
A microprocessor and heat sink may be hot if the system has been running. Also, there may be sharp pins and edges on some board and chassis parts. Contact should be made with care. Consider wearing protective gloves.

WARNING: English (continued)
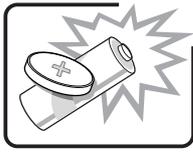
Danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the equipment manufacturer. Dispose of used batteries according to manufacturer's instructions.
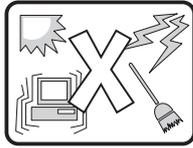
The system is designed to operate in a typical office environment. Choose a site that is:

- Clean and free of airborne particles (other than normal room dust).
- Well ventilated and away from sources of heat including direct sunlight.
- Away from sources of vibration or physical shock.
- Isolated from strong electromagnetic fields produced by electrical devices.
- In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppresser and disconnect telecommunication lines to your modem during an electrical storm.
- Provided with a properly grounded wall outlet.
- Provided with sufficient space to access the power supply cord(s), because they serve as the product's main power disconnect.

AVERTISSEMENT: Français
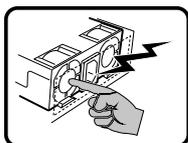
Le bloc d'alimentation de ce produit ne contient aucune pièce pouvant être réparée par l'utilisateur. Ce produit peut contenir plus d'un bloc d'alimentation. Veuillez contacter un technicien qualifié en cas de problème.
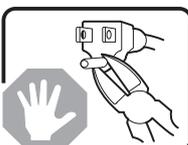
Ne pas essayer d'utiliser ni modifier le câble d'alimentation CA fourni, s'il ne correspond pas exactement au type requis. Le nombre de câbles d'alimentation CA fournis correspond au nombre de blocs d'alimentation du produit.
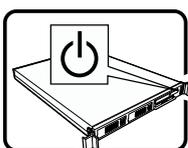
Notez que le commutateur CC de mise sous tension /hors tension du panneau avant n'éteint pas l'alimentation CA du système. Pour mettre le système hors tension, vous devez débrancher chaque câble d'alimentation de sa prise.

CONSIGNES DE SÉCURITÉ -Lorsque vous ouvrez le boîtier pour accéder à l'intérieur du système, suivez les consignes suivantes:

1. Mettez hors tension tous les périphériques connectés au système.
2. Mettez le système hors tension en mettant l'interrupteur général en position OFF (bouton-poussoir).
3. Débranchez tous les cordons d'alimentation c.a. du système et des prises murales.
4. Identifiez et débranchez tous les câbles reliés aux connecteurs d'E-S ou aux accès derrière le système.
5. Pour prévenir les décharges électrostatiques lorsque vous touchez aux composants, portez une bande antistatique pour poignet et reliez-la à la masse du système (toute surface métallique non peinte du boîtier).
6. Ne faites pas fonctionner le système tandis que le boîtier est ouvert.
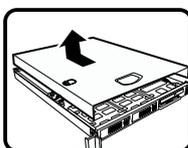
Une fois TOUTES les étapes précédentes accomplies, vous pouvez retirer les panneaux du système. Procédez comme suit:

1. Si un cadenas a été installé sur à l'arrière du système, déverrouillez-le et retirez-le.
2. Retirez toutes les vis des panneaux et mettez-les dans un endroit sûr.
3. Retirez les panneaux.
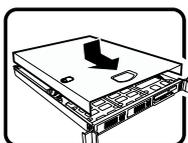
Afin de permettre le refroidissement et l'aération du système, réinstallez toujours les panneaux du boîtier avant de mettre le système sous tension. Le fonctionnement du système en l'absence des panneaux risque d'endommager ses pièces. Pour installer les panneaux, procédez comme suit:

1. Assurez-vous de ne pas avoir oublié d'outils ou de pièces démontées dans le système.
2. Assurez-vous que les câbles, les cartes d'extension et les autres composants sont bien installés.
3. Revissez solidement les panneaux du boîtier avec les vis retirées plus tôt.
4. Remettez le cadenas en place et verrouillez-le afin de prévenir tout accès non autorisé à l'intérieur du système.
5. Rebranchez tous les cordons d'alimentation c. a. et câbles externes au système.
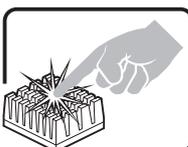
Le microprocesseur et le dissipateur de chaleur peuvent être chauds si le système a été sous tension. Faites également attention aux broches aiguës des cartes et aux bords tranchants du capot. Nous vous recommandons l'usage de gants de protection.

AVERTISSEMENT: Français (suite)
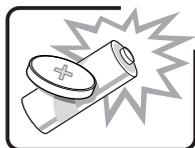
Danger d'explosion si la batterie n'est pas remontée correctement. Remplacer uniquement avec une batterie du même type ou d'un type équivalent recommandé par le fabricant. Disposez des piles usées selon les instructions du fabricant.
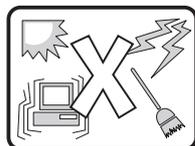
Le système a été conçu pour fonctionner dans un cadre de travail normal. L'emplacement choisi doit être:

- Propre et dépourvu de poussière en suspension (sauf la poussière normale).
- Bien aéré et loin des sources de chaleur, y compris du soleil direct.
- A l'abri des chocs et des sources de vibrations.
- Isolé de forts champs électromagnétiques géenérés par des appareils électriques.
- Dans les régions sujettes aux orages magnétiques il est recomandé de brancher votre système à un supresseur de surtension, et de débrancher toutes les lignes de télécommunications de votre modem durant un orage.
- Muni d'une prise murale correctement mise à la terre.
- Suffisamment spacieux pour vous permettre d'accéder aux câbles d'alimentation (ceux-ci étant le seul moyen de mettre le système hors tension).

WARNUNG: Deutsch
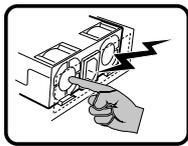
Benutzer können am Netzgerät dieses Produkts keine Reparaturen vornehmen. Das Produkt enthält möglicherweise mehrere Netzgeräte. Wartungsarbeiten müssen von qualifizierten Technikern ausgeführt werden.
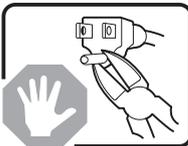
Versuchen Sie nicht, das mitgelieferte Netzkabel zu ändern oder zu verwenden, wenn es sich nicht genau um den erforderlichen Typ handelt. Ein Produkt mit mehreren Netzgeräten hat für jedes Netzgerät ein eigenes Netzkabel.
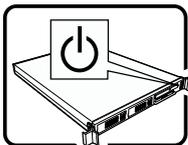
Der Wechselstrom des Systems wird durch den Ein-/Aus-Schalter für Gleichstrom nicht ausgeschaltet. Ziehen Sie jedes Wechselstrom-Netzkabel aus der Steckdose bzw. dem Netzgerät, um den Stromanschluß des Systems zu unterbrechen.
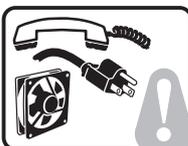
SICHERHEISMASSNAHMEN: Immer wenn Sie die Gehäuseabdeckung abnehmen um an das Systeminnere zu gelangen, sollten Sie folgende Schritte beachten:

1. Schalten Sie alle an Ihr System angeschlossenen Peripheriegeräte aus.
2. Schalten Sie das System mit dem Hauptschalter aus.
3. Ziehen Sie den Stromanschlußstecker Ihres Systems aus der Steckdose.
4. Auf der Rückseite des Systems beschriften und ziehen Sie alle Anschlußkabel von den I/O Anschlüssen oder Ports ab.
5. Tragen Sie ein geerdetes Antistatik Gelenkband, um elektrostatische Ladungen (ESD) über blanke Metallstellen bei der Handhabung der Komponenten zu vermeiden.
6. Schalten Sie das System niemals ohne ordnungsgemäß montiertes Gehäuse ein.
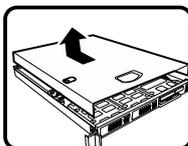
Nachdem Sie die oben erwähnten ersten sechs SICHERHEITSSCHRITTE durchgeführt haben, können Sie die Abdeckung abnehmen, indem Sie:

1. Öffnen und entfernen Sie die Verschlußeinrichtung (Padlock) auf der Rückseite des Systems, falls eine Verschlußeinrichtung installiert ist.
2. Entfernen Sie alle Schrauben der Gehäuseabdeckung.
3. Nehmen Sie die Abdeckung ab.
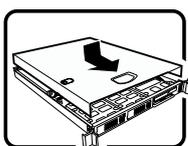
Zur ordnungsgemäßen Kühlung und Lüftung muß die Gehäuseabdeckung immer wieder vor dem Einschalten installiert werden. Ein Betrieb des Systems ohne angebrachte Abdeckung kann Ihrem System oder Teile darin beschädigen. Um die Abdeckung wieder anzubringen:

1. Vergewissern Sie sich, daß Sie keine Werkzeuge oder Teile im Innern des Systems zurückgelassen haben.
2. Überprüfen Sie alle Kabel, Zusatzkarten und andere Komponenten auf ordnungsgemäßen Sitz und Installation.
3. Bringen Sie die Abdeckungen wieder am Gehäuse an, indem Sie die zuvor gelösten Schrauben wieder anbringen. Ziehen Sie diese gut an.
4. Bringen Sie die Verschlußeinrichtung (Padlock) wieder an und schließen Sie diese, um ein unerlaubtes Öffnen des Systems zu verhindern.
5. Schließen Sie alle externen Kabel und den AC Stromanschlußstecker Ihres Systems wieder an.

Der Mikroprozessor und der Kühler sind möglicherweise erhitzt, wenn das System in Betrieb ist. Außerdem können einige Platinen und Gehäuseteile scharfe Spitzen und Kanten aufweisen. Arbeiten an Platinen und Gehäuse sollten vorsichtig ausgeführt werden. Sie sollten Schutzhandschuhe tragen.

Fortsetzung

WARNUNG: Deutsch (Fortsetzung)
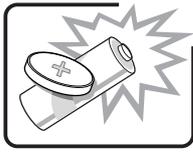
Bei falschem Einsetzen einer neuen Batterie besteht Explosionsgefahr. Die Batterie darf nur durch denselben oder einen entsprechenden, vom Hersteller empfohlenen Batterietyp ersetzt werden. Entsorgen Sie verbrauchte Batterien den Anweisungen des Herstellers entsprechend.
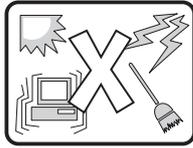
Das System wurde für den Betrieb in einer normalen Büroumgebung entwickelt. Der Standort sollte:

- sauber und staubfrei sein (Hausstaub ausgenommen);
- gut gelüftet und keinen Heizquellen ausgesetzt sein (einschließlich direkter Sonneneinstrahlung);
- keinen Erschütterungen ausgesetzt sein;
- keine starken, von elektrischen Geräten erzeugten elektromagnetischen Felder aufweisen;
- in Regionen, in denen elektrische Stürme auftreten, mit einem Überspannungsschutzgerät verbunden sein; während eines elektrischen Sturms sollte keine Verbindung der Telekommunikationsleitungen mit dem Modem bestehen;
- mit einer geerdeten Wechselstromsteckdose ausgerüstet sein;
- über ausreichend Platz verfügen, um Zugang zu den Netzkabeln zu gewährleisten, da der Stromanschluß des Produkts hauptsächlich über die Kabel unterbrochen wird.

AVVERTENZA: Italiano
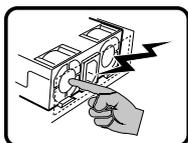
Rivolgersi ad un tecnico specializzato per la riparazione dei componenti dell'alimentazione di questo prodotto. È possibile che il prodotto disponga di più fonti di alimentazione.
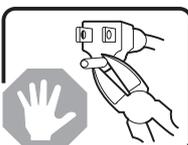
Non modificare o utilizzare il cavo di alimentazione in c.a. fornito dal produttore, se non corrisponde esattamente al tipo richiesto. Ad ogni fonte di alimentazione corrisponde un cavo di alimentazione in c.a. separato.
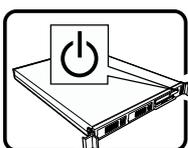
L'interruttore attivato/disattivato nel pannello anteriore non interrompe l'alimentazione in c.a. del sistema. Per interromperla, è necessario scollegare tutti i cavi di alimentazione in c.a. dalle prese a muro o dall'alimentazione di corrente.

PASSI DI SICUREZZA: Qualora si rimuovano le coperture del telaio per accedere all'interno del sistema, seguire i seguenti passi:

1. Spegnere tutti i dispositivi periferici collegati al sistema.
2. Spegnere il sistema, usando il pulsante spento/acceso dell'interruttore del sistema.
3. Togliere tutte le spine dei cavi del sistema dalle prese elettriche.
4. Identificare e sconnettere tutti i cavi attaccati ai collegamenti I/O od alle prese installate sul retro del sistema.
5. Qualora si tocchino i componenti, proteggersi dallo scarico elettrostatico (SES), portando un cinghia anti-statica da polso che è attaccata alla presa a terra del telaio del sistema – qualsiasi superficie non dipinta – .
6. Non far operare il sistema quando il telaio è senza le coperture.
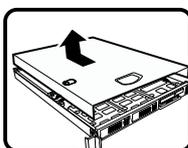
Dopo aver seguito i sei passi di SICUREZZA sopracitati, togliere le coperture del telaio del sistema come seque:

1. Aprire e rimuovere il lucchetto dal retro del sistema qualora ve ne fosse uno installato.
2. Togliere e mettere in un posto sicuro tutte le viti delle coperture.
3. Togliere le coperture.
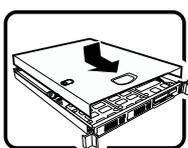
Per il giusto flusso dell'aria e raffreddamento del sistema, rimettere sempre le coperture del telaio prima di riaccendere il sistema. Operare il sistema senza le coperture al loro proprio posto potrebbe danneggiare i componenti del sistema. Per rimettere le coperture del telaio:

1. Controllare prima che non si siano lasciati degli attrezzi o dei componenti dentro il sistema.
2. Controllare che i cavi, dei supporti aggiuntivi ed altri componenti siano stati installati appropriatamente.
3. Attaccare le coperture al telaio con le viti tolte in precedenza e avvitarle strettamente.
4. Inserire e chiudere a chiave il lucchetto sul retro del sistema per impedire l'accesso non autorizzato al sistema.
5. Ricollegare tutti i cavi esterni e le prolunghe AC del sistema.
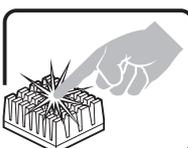
Se il sistema è stato a lungo in funzione, il microprocessore e il dissipatore di calore potrebbero essere surriscaldati. Fare attenzione alla presenza di piedini appuntiti e parti taglienti sulle schede e sul telaio. È consigliabile l'uso di guanti di protezione.

AVVERTENZA: Italiano (continua)
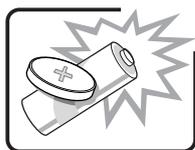
Esiste il pericolo di un esplosione se la pila non viene sostituita in modo corretto. Utilizzare solo pile uguali o di tipo equivalente a quelle consigliate dal produttore. Per disfarsi delle pile usate, seguire le istruzioni del produttore.
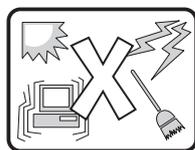
Il sistema è progettato per funzionare in un ambiente di lavoro tipo. Scegliere una postazione che sia:

- Pulita e libera da particelle in sospensione (a parte la normale polvere presente nell'ambiente).

- Ben ventilata e lontana da fonti di calore, compresa la luce solare diretta.

- Al riparo da urti e lontana da fonti di vibrazione.

- Isolata dai forti campi magnetici prodotti da dispositivi elettrici.

- In aree soggette a temporali, è consigliabile collegare il sistema ad un limitatore di corrente. In caso di temporali, scollegare le linee di comunicazione dal modem.

- Dotata di una presa a muro correttamente installata.

- Dotata di spazio sufficiente ad accedere ai cavi di alimentazione, i quali rappresentano il mezzo principale di scollegamento del sistema.

ADVERTENCIAS: Español
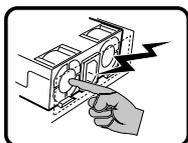
El usuario debe abstenerse de manipular los componentes de la fuente de alimentación de este producto, cuya reparación debe dejarse exclusivamente en manos de personal técnico especializado. Puede que este producto disponga de más de una fuente de alimentación.
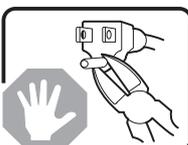
No intente modificar ni usar el cable de alimentación de corriente alterna, si no corresponde exactamente con el tipo requerido.

El número de cables suministrados se corresponden con el número de fuentes de alimentación de corriente alterna que tenga el producto.
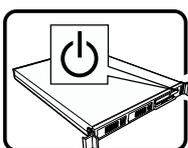
Nótese que el interruptor activado/desactivado en el panel frontal no desconecta la corriente alterna del sistema. Para desconectarla, deberá desenchufar todos los cables de corriente alterna de la pared o desconectar la fuente de alimentación.

INSTRUCCIONES DE SEGURIDAD: Cuando extraiga la tapa del chasis para acceder al interior del sistema, siga las siguientes instrucciones:

1. Apague todos los dispositivos periféricos conectados al sistema.
2. Apague el sistema presionando el interruptor encendido/apagado.
3. Desconecte todos los cables de alimentación CA del sistema o de las tomas de corriente alterna.
4. Identifique y desconecte todos los cables enchufados a los conectores E/S o a los puertos situados en la parte posterior del sistema.
5. Cuando manipule los componentes, es importante protegerse contra la descarga electrostática (ESD). Puede hacerlo si utiliza una muñequera antiestática sujetada a la toma de tierra del chasis — o a cualquier tipo de superficie de metal sin pintar.
6. No ponga en marcha el sistema si se han extraído las tapas del chasis.
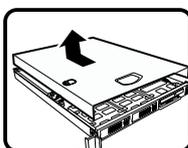
Después de completar las seis instrucciones de SEGURIDAD mencionadas, ya puede extraer las tapas del sistema. Para ello:

1. Desbloquee y extraiga el bloqueo de seguridad de la parte posterior del sistema, si se ha instalado uno.
2. Extraiga y guarde todos los tornillos de las tapas.
3. Extraiga las tapas.
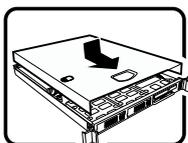
Para obtener un enfriamiento y un flujo de aire adecuados, reinstale siempre las tapas del chasis antes de poner en marcha el sistema. Si pone en funcionamiento el sistema sin las tapas bien colocadas puede dañar los componentes del sistema. Para instalar las tapas:

1. Asegúrese primero de no haber dejado herramientas o componentes sueltos dentro del sistema.
2. Compruebe que los cables, las placas adicionales y otros componentes se hayan instalado correctamente.
3. Incorpore las tapas al chasis mediante los tornillos extraídos anteriormente, tensándolos firmemente.
4. Inserte el bloqueo de seguridad en el sistema y bloquéelo para impedir que pueda accederse al mismo sin autorización.
5. Conecte todos los cables externos y los cables de alimentación CA al sistema.
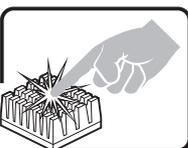
Si el sistema ha estado en funcionamiento, el microprocesador y el disipador de calor pueden estar aún calientes. También conviene tener en cuenta que en el chasis o en el tablero puede haber piezas cortantes o punzantes. Por ello, se recomienda precaución y el uso de guantes protectores.

ADVERTENCIAS: Español (continúa)
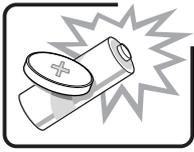
Existe peligro de explosión si la pila no se cambia de forma adecuada. Utilice solamente pilas iguales o del mismo tipo que las recomendadas por el fabricante del equipo. Para deshacerse de las pilas usadas, siga igualmente las instrucciones del fabricante.
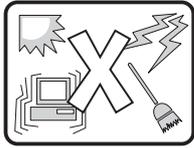
El sistema está diseñado para funcionar en un entorno de trabajo normal. Escoja un lugar:

- Limpio y libre de partículas en suspensión (salvo el polvo normal).
- Bien ventilado y alejado de fuentes de calor, incluida la luz solar directa.
- Alejado de fuentes de vibración.
- Aislado de campos electromagnéticos fuertes producidos por dispositivos eléctricos.
- En regiones con frecuentes tormentas eléctricas, se recomienda conectar su sistema a un eliminador de sobrevoltage y desconectar el módem de las líneas de telecomunicación durante las tormentas.
- Provisto de una toma de tierra correctamente instalada.
- Provisto de espacio suficiente como para acceder a los cables de alimentación, ya que éstos hacen de medio principal de desconexión del sistema.

Vos remarques sur ce document / Technical publication remark form

Titre / Title :   Bull NovaScale 4020 User's Guide

Nº Reférence / Reference Nº :   86 A1 72EG 01

Daté / Dated :   February 2004

ERREURS DETECTEES / ERRORS IN PUBLICATION

AMELIORATIONS SUGGEREES / SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

Vos remarques et suggestions seront examinées attentivement.
Si vous désirez une réponse écrite, veuillez indiquer ci-après votre adresse postale complète.

Your comments will be promptly investigated by qualified technical personnel and action will be taken as required.
If you require a written reply, please furnish your complete mailing address below.

NOM / NAME : _____   Date : _____

SOCIETE / COMPANY : _____

ADRESSE / ADDRESS : _____

_____

Remettez cet imprimé à un responsable BULL ou envoyez-le directement à :

Please give this technical publication remark form to your BULL representative or mail to:

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

Technical Publications Ordering Form

Bon de Commande de Documents Techniques

To order additional publications, please fill up a copy of this form and send it via mail to:
Pour commander des documents techniques, remplissez une copie de ce formulaire et envoyez-la à :

BULL CEDOC
ATTN / Mr. L. CHERUBIN   **Phone** / Téléphone :   +33 (0) 2 41 73 63 96
357 AVENUE PATTON   **FAX** / Télécopie   +33 (0) 2 41 73 60 19
B.P.20845   **E–Mail** / Courrier Electronique :   srv.Cedoc@franp.bull.fr
49008 ANGERS CEDEX 01
FRANCE

Or visit our web sites at: / Ou visitez nos sites web à:
http://www.logistics.bull.net/cedoc
`http://www-frec.bull.com`   `http://www.bull.com`

CEDOC Reference # Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté
_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]	
_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]	
_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]	
_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]	
_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]	
_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]	
_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]	

[_ _] :   **no revision number means latest revision** / pas de numéro de révision signifie révision la plus récente

NOM / NAME : _____   Date : _____

SOCIETE / COMPANY : _____

ADRESSE / ADDRESS : _____

_____

PHONE / TELEPHONE : _____   FAX : _____

E–MAIL : _____

For Bull Subsidiaries / Pour les Filiales Bull :

Identification: _____

For Bull Affiliated Customers / Pour les Clients Affiliés Bull :

Customer Code / Code Client : _____

For Bull Internal Customers / Pour les Clients Internes Bull :

Budgetary Section / Section Budgétaire : _____

For Others / Pour les Autres :

Please ask your Bull representative. / Merci de demander à votre contact Bull.

Utiliser les marques de découpe pour obtenir les étiquettes.
Use the cut marks to get the labels.

NovaScale
4020
User's Guide

86 A1 72EG 01