Intel® Server Boards and Server Platforms Server Management Guide

Intel part number: G37830-001

Revision History

Revision History

Date	Revision	Description
March 2008	0.5	Initial release.
April 2008	0.9	Updated it for all currently shipping servers.
March 2009	1.0	Overhauled the entire document.
September 2009	1.1	Added S3420GP support.
June 2011	2.0	Added S1200BT support.

Table of Contents

List of Figures

List of Tables

<This page is intentionally left blank.>

1   Introduction

The server management hardware that is part of Intel® server boards and Intel® server platforms serves as a vital part of the overall server management strategy. The server management hardware provides essential information to the system administrator and provides the administrator the ability to remotely control the server, even when the operating system is not running.

The Intel® server boards and Intel® server platforms offer comprehensive hardware and software based solutions. The server management features make the servers simple to manage and provide alerting on system events. From entry to enterprise systems, good overall server management is essential to reducing overall total cost of ownership.

This User's guide covers the hardware-based server management solutions offered on Intel® server boards and Intel® server platforms, specifically the embedded Baseboard Management Controller (BMC).

There is a separate user's guide that covers the server management software offered on Intel® server boards and Intel® Server platforms.

1.1   Industry standards

1.1.1   Intelligent Platform Management Interface (IPMI)

The key characteristic of the Intelligent Platform Management Interface (IPMI) is that the inventory, monitoring, logging, and recovery control functions are available independent of the main processors, BIOS, and operating system. Platform management functions can also be made available when the system is in a powered down state.

IPMI works by interfacing with the BMC, which extends management capabilities in the server system and operates independent of the main processor by monitoring the on-board instrumentation. Through the BMC, IPMI also allows administrators to control power to the server, and remotely access BIOS configuration and operating system console information.

IPMI defines a common platform instrumentation interface to enable interoperability between:

- The baseboard management controller and chassis.
- The baseboard management controller and systems management software
- Between servers.

IPMI enables the following:

- Common access to platform management information, consisting of:
    − Local access through systems management software
    − Remote access through LAN
    − Inter-chassis access through Intelligent Chassis Management Bus

- − Access through LAN, serial/modem, IPMB, PCI SMBus, or ICMB, available even if the processor is down
- IPMI interface isolates systems management software from hardware.
- Hardware advancements can be made without impacting the systems management software.
- IPMI facilitates cross-platform management software.

You can find more information on IPMI at the following URL: http://www.intel.com/design/servers/ipmi.

1.1.2   Baseboard Management Controller (BMC)

A baseboard management controller (BMC) is a specialized microcontroller embedded on most Intel® Server Boards. The BMC is the heart of the IPMI architecture and provides the intelligence behind intelligent platform management, that is, the autonomous monitoring and recovery features implemented directly in platform management hardware and firmware.

Different types of sensors built into the computer system report to the BMC on parameters such as temperature, cooling fan speeds, power mode, operating system status, etc. The BMC monitors the system for critical events by communicating with various sensors on the system board; it sends alerts and logs events when certain parameters exceed their preset thresholds, indicating a potential failure of the system. The administrator can also remotely communicate with the BMC to take some corrective action such as resetting or power cycling the system to get a hung OS running again. These abilities save on the total cost of ownership of a system.

For Intel® server boards and Intel® Server platforms, the BMC supports the industry-standard IPMI 2.0 specification, enabling you to configure, monitor, and recover systems remotely.

1.1.3   Add-on Management Module (RMM) advanced features

Apart from BMC basic functions embedded along with Intel® Server Boards. The customer has an option to add-on Remote Management Module (RMM) to Intel® Server boards. Then the customers can gain advanced features as like Remote KVM and Remote Media.

1.2   Management features supported in Intel® Server Boards

With embedded BMC, Intel® Server Boards or Intel® Server platforms are able to provide the following system management monitoring and control features:

- **In-band or Out-of-band communication**

IPMI provides either in-band or out-of-band (OOB) communication to the computer hardware and firmware, which system administrators can use to monitor system health and manage the system.

- In-Band

This involves communicating to the BMC by utilizing the OS services through server management software agents. This provides an enhanced level of manageability by providing in-band access to the IPMI management information and integrating IPMI with the additional management functions provided by management applications and the OS. System management software such as Intel® System Management Software and the OS can provide a more sophisticated control, error handling and alerting, than can be directly provided by the platform management subsystem.

- Out-of-Band (OOB)

This involves communicating directly to the BMC and bypassing the OS.

Platform status information can also be obtained and recovery actions can be initiated under situations where the system management software and normal 'in-band' management mechanisms are unavailable.

- **System Event Log (SEL)**

The BMC provides a centralized, non-volatile repository for critical, warning, and informational system events called the System Event Log or SEL. By having the BMC manage the SEL and logging functions, it helps to ensure that 'post-mortem' logging information is available should a failure occur that disables the systems processor(s).

The BMC allows access to SEL through in-band and out-of-band mechanisms. The tools or utilities are as like Intel® SELViewer and open sourced ipmitool.

- **Asset information (FRU information)**

The BMC provides access to non-volatile asset\inventory data of major system components called Field Replaceable Unit (FRU) information. Access to FRU information provides vital data such as serial numbers and part numbers for various replaceable boards and other components.

The BMC allows access to FRU through in-band and out-of-band mechanisms.

- **Sensor Monitoring**

The BMC provides monitoring and control of system sensors. The BMC polls system sensors to monitor and report system health. These sensors include soft sensors that are used for reporting system state and events, and hardware sensors. The most popular forms of monitoring are System voltage monitoring, System temperature monitoring, system fans and power supplies monitoring.

The BMC allows access to sensor data through in-band and out-of-band mechanisms.

- **Fan speed control and Fan speed monitoring**

The BMC monitors and controls the system fans. For each fan, a fan speed sensor provides fan failure detection. Some systems provide fan presence detection in which the BMC maps into per-fan presence sensors. The BMC can control the speed of some fans. Controllable fans are divided into fan domains in which there is a separate fan speed control for each domain and a separate fan control policy configurable for each domain.

A fan domain can have a set of temperature and fan sensors associated with it. These are used to determine the current fan domain state. A fan domain has three states: sleep, nominal, and boost.

- **Remote management through LAN**

Remote management through LAN is made possible by IPMI over LAN, which used to transfer IPMI messages between the Baseboard Management Controller and remote management software through a side-band channel redirected from the NIC to the BMC. The BMC has its own Media Access Control (MAC) address and IP address, which are different from the MAC address and IP address shown by the OS.

Before IPMI messaging can work on a LAN connection, administrators must enable\configure the system for IPMI over LAN mode. By default, the IPMI over LAN mode is disabled to prevent unauthorized access. However, even if IPMI over LAN is disabled, other related attributes can still be configured through Server Administrator and will take effect whenever IPMI over LAN is finally enabled.

From the IPMI point-of-view, the interface to the network controller is dedicated to the BMC. That is, there are no special commands for coordinating the sharing of the network controller between system software access and BMC access, as there are with Serial Port Sharing.

BMC provides the following features through IPMI over LAN:

- Remote power on\off\reset
- Access to SEL
- Access to FRU (asset information)
- Access to system sensor data
- **Serial over LAN (SOL)**

Another key IPMI feature of OOB is the text-based console redirection through Serial over LAN (SOL). Serial over LAN (SOL) is the name for the redirection of baseboard serial controller traffic over an IPMI session. The SOL feature provides remote connection to the system serial console.

SOL can be used to provide a user at a remote console a means to interact with serial text-based interfaces such as operating system command-line interfaces, serial redirected BIOS interfaces, and serial text-based applications over an IPMI LAN session. A single remote console application can use SOL to simultaneously provide LAN access to IPMI platform management and serial text redirection under a unified user interface. For example, access to Red Hat* Enterprise Linux serial console interfaces by using serial over LAN.

Access privileges for SOL are managed under the same user configuration interfaces that are used for IPMI management. This simplifies the creation of configuration software, remote management applications, and cross-platform configuration utilities.

Before SOL can work on a LAN connection, administrators must enable the system for SOL. By default, SOL is disabled to prevent unauthorized access.

- **Alerting**

BMC supports two types of alerts: SNMP traps also called LAN alerts, and Email Alerts. Both alerts can be configured using the Intel® Deployment Assistant or System configuration utility.

- **SNMP Traps (LAN alerts)**

BMC supports LAN Alerting in the form of Small Network Management Protocol (SNMP) Traps that

follows the Platform Event Trap (PET) format. SNMP Traps are typically sent as unreliable datagrams. However, IPMI includes PET Acknowledge and retry options that allow an IPMI-aware remote application to provide a positive acknowledge that the trap was received.

Alert-over-LAN notifies remote system management application about Platform Event filter (PEF) selected events, regardless of the state of the server's operating system. LAN alerts can be sent over any of the LAN channels supported by a system.

- **Email Alerts**

BMC supports Email alerting through the Simple Mail Transport Protocol (SMTP). This feature allows the user to receive Email alerts indicating issues with the server. The email alert provides a text string that describes a simple description of the event.

- **Power Management**

Intel® S5500 Series Server Boards support power management through the Intel® Node Manager technology. It is a platform-resident technology that enforces power policies for the platform. These policies are applied by exploiting subsystem knobs (such as processor P and T states) that can be used to control power consumption. Node Manager enables data center power management by exposing an external interface to management software through which platform power policies can be specified.

The Intel® Node manager technology on EPSD platforms can

- Monitor and report platform power consumption
- Control total system power consumption by using P-State\C-State cycling method
- Enforce user-defined policies and actions
    - Set power limit for a system within a specified activation period
    - Report exceptions when power limit cannot be met by the system
    - Initiate power-off action when power limit cannot be met by the system
- Does not require any additional OS driver
    - Utilizes OS Power Management in Advanced Configuration and Power Interface (ACPI)-compliant systems

Intel® S5500 Series server boards and platforms do not support temperature-based power policies.

- **Systems Management Architecture for Server Hardware (SMASH) command line protocol or (CLP) Basic**

The goal of the SMASH CLP is to reduce management complexity by delivering a human-oriented interface that provides a uniform command set to control hardware. The CLP allows users to execute common operations such as system power on and off, display hardware event logs, or view sensor information.

- Power control:

    System Reset: `reset system1`

    Power Off: `stop /system1`

Power On: `start /system1`

- Display SEL:

Display a list of records: `show /system1/log1`

Display individual record: show /system1/log1/record<nnn>

Example: show /system1/log1/record33

- Display sensor information:

Display a list of sensors: `show /system1`

Display a sensor: show /system1/<sensor name from sensor list>

Example: show /system1/sensor25

show /system1/tempsensor1

1.3   Advanced Management features of Intel® RMM2/RMM3/RMM4 solutions

Intel Remote Management Module (RMM2/3/4) is add-on solutions to enhance baseboard management controller on Intel server boards. With this option, the customer can get Remote KVM and Remote Video features when doing Server remote management:

On different generation Intel Server boards, we have different RMM solutions:

- RMM2 is for Intel Server S5000 series platforms
- RMM3 is for Intel Server S5500 series platforms
- RMM4 is for Intel Server S1200BT series platforms

2 Baseboard Management Controller

2.1 Feature comparison between different generation Intel® Server Boards

Different generations of Intel® Server boards have a different type of BMC integrated onto the server boards. Also, different generations of Intel® Server boards only support different types of add-on remote management cards.

The level of monitoring and alerting features provided depend on the type of on-board BMC and add-on remote management card.

The key differences between on-board BMC and add-on remote management card are remote media and remote KVM functions.

This chapter describes these on-board and add-on remote management cards, including communication methods, features, functionality, cabling, and configuration of each. The following are discussed here:

- The ESB2 BMC used in Intel® S5000 series server boards and Intel® S7000 series server boards.
- The Integrated BMC used in Intel® S5500 series server boards.
- The Integrated BMC used in Intel® S1200BT series server boards.

The mini-BMC is found only in Intel® SE7520 server boards. For more information on this device, refer to related documents on previous generations of Intel® Server boards.

The following table shows the key differential on manageability features between different kinds of BMC and add-on remote management cards:

Table 1. Feature Comparison

Manageability features	Intel® S5000/S7000 Server Boards	Intel® S3200/X38ML Server Boards	Intel® S5500/S3420 Server Boards	Intel® S1200BT Server Boards
IPMI Support	2.0	2.0	2.0	2.0
System Event log (3276 records)	Yes	Yes	Yes	Yes
Asset information (FRU information)	Yes	Yes	Yes	Yes
Sensor Monitoring: voltage, temperature, fans, power supply	Yes	Yes	Yes	Yes
Fan speed control	Yes	Yes	Yes	Yes
Remote management through LAN: Remote power on\off\reset, read SEL,	Yes	Yes	Yes	Yes

Baseboard Management Controller

Manageability features	Intel® S5000/S7000 Server Boards	Intel® S3200/X38ML Server Boards	Intel® S5500/S3420 Server Boards	Intel® S1200BT Server Boards
Sensor status (system health)				
Serial Over LAN (Console redirection over LAN)	Yes	Yes	Yes	Yes
SNMP traps (LAN alerts) and Platform Event Filtering	Yes	Yes	Yes	Yes
Email Alerts	Yes	N/A	Yes	Yes
Remote Management through serial port	Yes	N/A	Yes	Yes
Auto recovery from hangs during boot – BMC watchdog timer	Yes	Yes	Yes	Yes
Power management(Power capping through Node Manager based on PMBus)	N/A	N/A	Yes	Yes
SMASH CLP Basic: Remote Power on\off\reset, display SEL and sensor status, SSH to SOL, turn on\off chassis ID LED	Yes	Yes	Yes	Yes
Remote KVM Support	Support with Intel® RMM2	N/A	Support with Intel® RMM3	Support with Intel® RMM4
Remote Media Support	Support with Intel® RMM2	N/A	Support with Intel® RMM3	Support with Intel® RMM4

For a quick overview on differences between BMC types, the key features are listed in the following table:

Table 2. Key differences Between BMC features

	Intel® S5000/S7000 Server Boards	Intel® S3200/X38ML Server Boards	Intel® Server Board S5500BC	Intel® Server Boards S5500HC/S5520SC/ S5520UR/SC5520W B/S3420GP	Intel® Server Boards S1200BT
IPMI	IPMI 2.0	IPMI 2.0	IPMI 2.0	IPMI 2.0	IPMI 2.0
Channels	7 defined channels 2 NIC 1 serial	3 defined channels 1 NIC	7 channels 2 NIC 1 Serial 1 USB	7 channels 2 NIC 1 Serial 1 USB	7 channels 2 NIC 1 Serial 1 USB
MAC	Dedicated MAC for management	Dedicated MAC for management	Dedicated MAC for management	Dedicated MAC for management	Dedicated MAC for management
External Connection (Shared)	NIC1 and NIC2	NIC1	NIC2	NIC1	NIC1
Users	15 users 1 null 14 custom	15 users 1 null 4 predefined 10 custom	15 users 1 null 4 predefined 10 custom	15 users 1 null 4 predefined 10 custom	15 users 1 null 4 predefined 10 custom
IPMI Sessions	5 simultaneous sessions	4 simultaneous sessions	IPMI-over-LAN – 5 sessions WebServer – 4 sessions KVM/Media redirect – 2 sessions Serial – 1 session	IPMI-over-LAN – 5 sessions WebServer – 4 sessions KVM/Media redirect – 2 sessions Serial – 1 session	IPMI-over-LAN – 5 sessions WebServer – 4 sessions KVM/Media redirect – 2 sessions Serial – 1 session
Management Module	Intel® RMM2	No	Intel® RMM3	Intel® RMM3	Intel® RMM4

✏ **NOTE**

IPMI LAN channel may be switched to either NIC depending on platform. For additional information, refer to the *Technical Product Specification (TPS)* for individual products.

For a detailed comparison between ESB2 BMC and Integrated BMC based Intel Servers, read through sections 2.2 through section 2.5.

2.2   BMC in Intel® S5000/S7000 Server Boards

2.2.1   LAN interface

Intel® S5000 Server boards are embedded with ESB2 BMC that implements both the IPMI 1.5 and IPMI 2.0 messaging models. These provide out-of-band local area network (LAN) communication between the

BMC and the external world.

The BMC supports a maximum of three LAN interfaces:

- Two LAN interfaces utilize the embedded ESB2 NICs (one channel per embedded NIC).
- One LAN interfaces utilizes an optional external NIC known as the ASMI NIC. Use of this NIC requires the installation of the optional Intel® Remote Management Module add-in card.

Run-time determination of LAN channel capabilities can be made both by standard IPMI defined mechanisms and by an OEM configuration parameter that defines advanced feature support.

2.2.2   ESB2 Embedded LAN Channels

Even though the ESB2 embedded NICs are shared by the BMC and the server, sharing only means that both the BMC and the server use the same NIC. These shared NICs provide a dedicated MAC address solely for BMC use. As a result, in some ways these channels are more similar to a dedicated LAN channel than a shared channel.

For these channels, support can be enabled for IPMI-over-LAN, ARP, and DHCP. As an integral part of the ESB2, the BMC has a high degree of access to and control over its primary network interfaces.

If an Intel® Remote Management Module 2 add-in card is installed, the ESB2 embedded LAN channels are typically configured differently than for a server that does not include this device.

Channels 1-7 can be assigned to different types of communication media and protocols for IPMI messages (for example, IPMB, LAN, ICMB, etc.), based on the system implementation.

2.2.3   IPMI 2.0 Channel Management

Every messaging interface is assigned an IPMI channel ID by IPMI 2.0. Commands are provided to configure each channel for privilege levels and access modes.

Channels 1-7 can be assigned to different types of communication media and protocols for IPMI messages (for example, IPMB, LAN, ICMB, etc.), based on the system implementation.

Table 3. Standard Channel Assignments

Channel ID	Interface	Supports Sessions
0	IPMB	No
1	LAN 1 (ESB2 NIC)	Yes
2	LAN 2 [1] (ESB2 NIC)	Yes
3	LAN 3 [1] (Intel Remote Management Module 2)	No
4	EMP (Basic/PPP)	Yes
5	Reserved	–
6	PCI SMBus	–
7	SMM	No
0Eh	Self	–
0Fh	SMS/Receive Message Queue	No

Note: If supported by the server system.

2.2.4 Dedicated MAC Address

Each of the ESB2's two NIC channels has a unicast MAC filter reserved for BMC use. These filters enable the BMC to receive network data streams that are logically separate from, and invisible to, operating systems and software running on the server, despite sharing the same physical LAN connections. This allows the BMC to support features beyond standard IPMI-over-LAN, such as DHCP, full ARP request/response, and ICMP, without requiring a separate Ethernet cable.

For Intel® S5000 series server boards, each server board has four MAC addresses assigned to it at the Intel factory. The printed MAC address is assigned to NIC1 on the server board.

- NIC 1 MAC address (for OS usage)
- NIC 2 MAC address = NIC 1 MAC address + 1 (for OS usage)
- BMC LAN channel 1 MAC address = NIC1 MAC address + 2
- BMC LAN channel 2 MAC address = NIC2 MAC address + 2

2.2.5 BMC IP Address and external connection

The BMC IP address for a particular embedded NIC is always different from the IP address of the Server's OS.

The BMC IP address can be either a static IP address or a DHCP-sourced IP address.

The BMC communicates through NIC 1 or NIC 2 depending on your network configuration. To communicate with the BMC, you need to attach a standard Ethernet cable. You cannot use PING to confirm that this connection is valid.

✏️ **NOTE**

Only one dedicated interface can be enabled for management traffic at any time.

For details on which Ethernet port is shared with the BMC to ensure successful communication, see the following table.

Table 4. Shared Ethernet ports with BMC

Intel® Server Boards	System Ethernet port shared with the BMC
Intel® S5000 Server Boards	On-board NIC1 or NIC 2
Intel® S7000 Server Boards	On-board NIC1 or NIC 2

✏️ **NOTE**

Intel® S3000 Server Boards does not have an on-board BMC. Its management function is based on Intel® Advanced Management Technology (AMT). For detailed information, refer to the Intel® S3000 Server Board Technical Product Specification (TPS).

The following figure displays the location for NIC1 and NIC2 on Intel® Server System SR2500 to serve as a reference.

✏️ **NOTE**

The location of the on-board NICs may be slightly different on other Intel® Server boards.

A	On-board NIC1
B	On-board NIC2
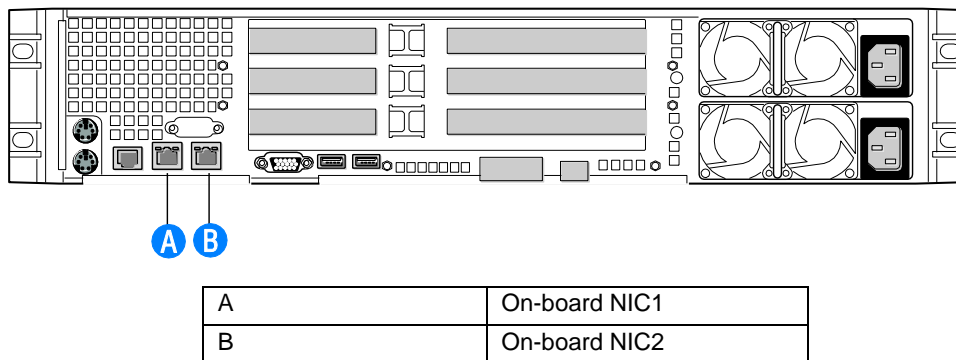
Figure 1. Rear connectors of the Intel® Server System SR2500

2.2.6 BMC Users

The BMC supports the IPMI 2.0 user model, including 15 User IDs on ESB2-based Intel® Server boards and systems. These 15 users can be assigned to any channel.

Table 5. BMC Users

Users	User Name	Password	Status	Characteristics
User 1	Null	Null	Disabled	Only Password can be changed.
User 2	root	Superuser	Disabled	Only Password can be changed.
User 3	test1	Superuser	Disabled	User name and password can be changed.
User 4	test2	Superuser	Disabled	User name and password can be changed.
User 5	test3	Superuser	Disabled	User name and password can be changed.
User 6-15	undefined	undefined	Disabled	User name and password can be changed.

Intel® recommends changing the password if using user 1 or 2, and changing both user name and password if using user 3-5.

2.2.7   Session Support

The BMC supports five simultaneous sessions, shared across all session-based channels.

2.2.8   Intel® Remote Management Module 2

The Intel® RMM2 offers convenient, remote KVM access and control across the LAN or through the Internet. It captures, digitizes, and compresses video and transmits it with keyboard and mouse signals to and from a remote computer. Remote access and control software runs on Intel® RMM2 embedded processors so there is no impact to the server operation or network performance. In addition, the Intel® RMM2 offers integrated remote power management using IPMI.

Key features of the Intel® RMM2 add-on card are:

- Embedded Web UI – Remote Power on\off, system health, system information, Intel® RMM2 Firmware Update, Event log includes Intel® RMM2 events

- KVM redirection through Dedicated NIC – high performance, multiple concurrent sessions

- USB 2.0 media redirection – boot over remote media

- Security – SSL, LDAP, SSH, RADIUS support

- Email Alerting for Intel® RMM2 events

- SMASH CLI/CLP, Web Services for Management (WS-MAN), SNMP traps for Intel® RMM2 events

- Soft Keyboard through KVM (Multiple Language support)

- IPMI V2.0 Compliance

- Allows remote viewing and configuration in pre-boot POST and BIOS setup

Figure 2. Intel® Remote Management Module 2 and NIC

Intel® RMM2 contains a dedicated NIC that is able to support both DHCP and static IP addresses. RMM2 has its own user authorization solution that is not similar to BMC's user authorization.

Intel® RMM2 has several utilities to perform network and user configuration.

The Intel® RMM2 module features an embedded operating system and applications that offer a variety of standardized interfaces. You can access the Intel® RMM2 using the unsecured HTTP protocol or using the encrypted HTTPS protocol; HTTPS is preferred.

For detailed information on how to configure and use Intel® RMM2, refer to Intel® RMM2 User Guide that is available at http://www.intel.com/

2.2.9   Access BMC through Intel® RMM2

The Intel® RMM2 is IPMI V2.0 compliant. It allows the customer to remote access BMC through Intel® RMM2's dedicated LAN channel (LAN channel 3)

- Intel® RMM2 supports the IPMI forwarding function. The customer can send IPMI commands through the dedicated NIC on the Intel® RMM2.

- Intel® RMM2 also supports SOL over this channel. The customer can activate SOL session through the dedicated NIC on the Intel® RMM2.

To perform these features, you need to enable the BMC account first. At this point, BMC (not RMM2) handles the authorization, so use the BMC account and password in the IPMI based command.

Examples on step by step instructions:

1. Update both Intel® RMM2 and system's BMC FW to the latest
2. Use psetup or kiratool to setup Intel® RMM2's IP address (static or DHCP)
3. Use SYSCFG utility to configure BMC users and BMC LAN channel 3 setting:
   > syscfg /u 3 admin password   # configure user 3's user name and password
   > syscfg /ue 3 enable 3   # enable user 3 on LAN channel 3
   > syscfg /up 3 3 admin   # assign user 3 with admin privilege on LAN channel 3
   > syscfg /c 3 7 always   # configure LAN channel 3 access mode to "Always"
4. Configure IPMI forwarding from Intel® RMM2's web GUI as following:

Figure 3. IPMI channel 3 settings on Intel® RMM2 navigation web page

➲   **NOTE**

You can also enable SOL function per your configuration.

5. Restart RMM2 by doing:
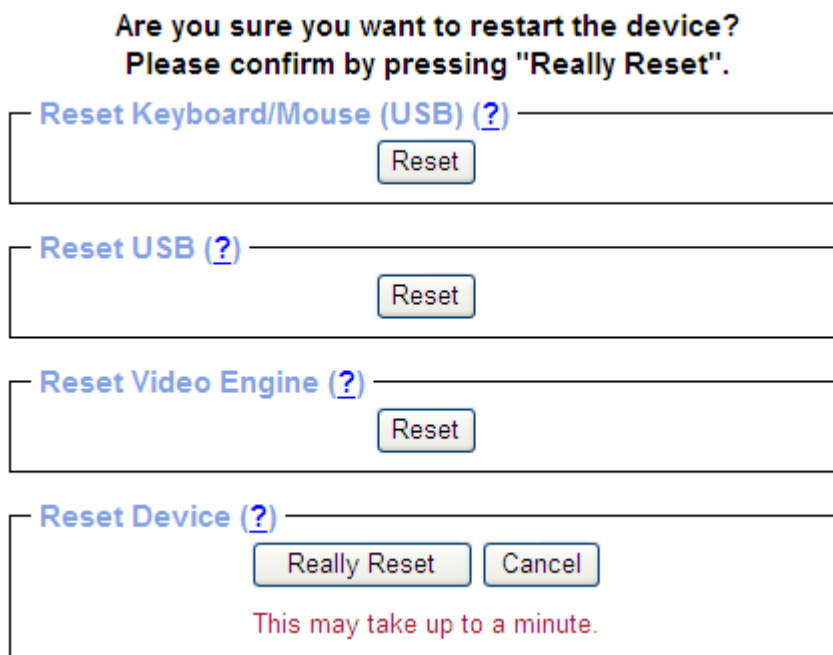
Figure 4. Restart RMM2

6. Check/confirm RMM2's IP address by psetup or kiratool (DHCP IP address could be changed after RMM2 reset)
7. Restart BMC by doing:
   > syscfg /rbmc
8. User IPMITOOL to access BMC through Intel® RMM2's dedicate NIC:
   > ipmitool -I lan -H 10.239.56.103 -U "admin" -P "password" fru

✏ **NOTE**

Here "10.239.56.103" is an example of Intel® RMM2's IP address. Your BMC's configuration about user name and IP address may be varied.

2.3 BMC in Intel® S3200/X38ML Server Boards

2.3.1 LAN interface

Intel® S3200/X38ML Server boards are embedded with Integrated BMC. The BMC implements both the IPMI 1.5 and IPMI 2.0 messaging models. These provide out-of-band local area network (LAN) communication between the BMC and the external world.

The BMC supports a maximum of one LAN interface:

- Intel® Server Board S3200SH and Intel® Server Board X38ML support two LAN interfaces for operating system use but only NIC1 is able to handle BMC server management traffic.

2.3.2 IPMI 2.0 Channel Management

Every messaging interface is assigned an IPMI channel ID by IPMI 2.0. Commands are provided to configure each channel for privilege levels and access modes. The following table shows the standard channel assignments.

Table 6. Standard Channel Assignments

Channel ID	Interface	Supports Sessions
0	IPMB	No
1	LAN 1	Yes
4	Reserved	–
5	Reserved	–
6	Reserved	–
7	SMM	No
0Eh	Self	–
0Fh	SMS/Receive Message Queue	No

2.3.3 Dedicated MAC Address

The Integrated BMC share the same physical Ethernet link with system's on-board NIC1. These filters enable the BMC to receive network data streams that are logically separate from, and invisible to, operating systems and software running on the server, despite sharing the same physical LAN connections. This allows the BMC to support features beyond standard IPMI-over-LAN, such as DHCP, full ARP request/response, and ICMP, without requiring a separate Ethernet cable.

For Intel® Server Board S3200SH and Intel® Server Board X38ML, the server board supports two LAN interfaces for operating system use but only NIC1 supports the handling of server management traffic as BMC host IP Address.

- NIC 1 MAC address (for OS usage)
- NIC 2 MAC address = NIC 1 MAC address + 1 (for OS usage)
- BMC LAN channel 1 MAC address = NIC1 MAC address +2

2.3.4 BMC IP Address and external connection

The BMC IP address for a particular embedded NIC is always different from the IP address of the Server's OS.

The BMC IP address can either be a static IP address or DHCP sourced IP address.

The Integrated BMC communicates through NIC 1 only. To communicate with the BMC, you need to attach a standard Ethernet cable. You cannot use PING to confirm that this connection is valid.

For details on which Ethernet port is shared with the BMC to ensure successful communication, see the following table.

Table 7. Shared Ethernet ports with BMC

Intel® Server Boards	System Ethernet port shared with the BMC
Intel® S3200 Server Boards	On-board NIC1
Intel® Server Board X38ML	On-board NIC1

The following figure displays the location for NIC1 and NIC2 on Intel® Server System SR1520ML to serve as a reference.

✏ **NOTE**

The location of the on-board NICs may be slightly different on other Intel® server boards.

A	On-board NIC1
B	On-board NIC2
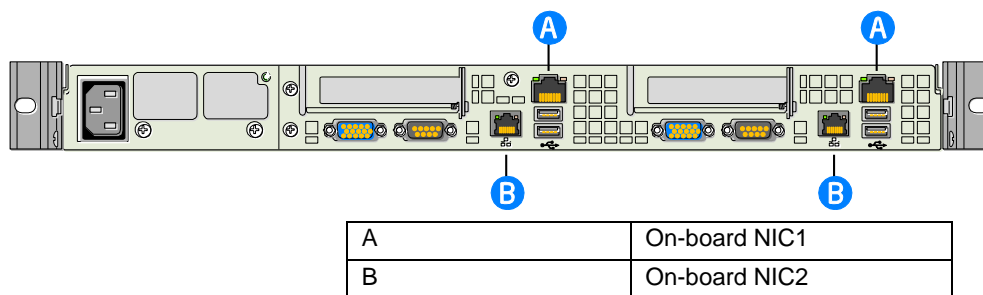
Figure 5. Rear connectors of the Intel® Server System SR1520ML

2.3.5 BMC Users

The BMC supports the IPMI 2.0 user model, including *User ID 1* support. 15 user IDs are supported. These 15 users can be assigned to any channel. The following restrictions are placed on user-related operations:

- User names for User IDs 1 and 2 cannot be changed. These will always be "" (Null) and "root" respectively.
- User 2 ("root") will always have the administrator privilege level.
- All user passwords (including passwords for User 1 and User 2) may be modified.
- User IDs 3-15 may be used freely, with the condition that user names are unique. Therefore, no other users can be named as "" (Null), "root," or any other existing user name.

Table 8. Feature Comparison

Users	User Name	Password	Status	Characteristics
User 1	Null	Null	Disabled	Only Password can be changed.
User 2	root	superuser	Disabled	Only Password can be changed.
User 3	test1	superuser	Disabled	Both user name and password can be changed.
User 4	test2	superuser	Disabled	Both user name and password can be changed.
User 5	test3	superuser	Disabled	Both user name and password can be changed.
User 6-15	undefined	undefined	Disabled	Both user name and password can be changed

Intel® recommends changing the password if using user 1 or 2, and changing both user name and password if using user 3-5.

2.3.6 Session Support

The BMC supports a maximum of four simultaneous sessions. This is shared across all session-based channels. The BMC also supports multiple sessions on a given channel.

2.4 BMC in Intel® S5500/S3420 Server Boards

2.4.1 LAN interface

Intel® S5500 Server Boards are embedded with the Integrated BMC. The Integrated BMC implements both the IPMI 1.5 and IPMI 2.0 messaging models. These provide out-of-band local area network (LAN) communication between BMC and the network.

2.4.2 BMC Embedded LAN Channels

BMC hardware includes two dedicated 10/100 network interfaces:

- **Interface 1:** This interface is available from the on-board NIC ports in a system, which can be shared with the host. Only one NIC may be enabled for management traffic at any time.

- **Interface 2:** This interface is available from Intel® RMM3, which is a dedicated management NIC and not shared with the host.

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

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

- IP Address: Static

- All users disabled

IPMI-enabled network interfaces may not be placed on the same subnet. This includes the Intel® RMM3's on-board network interface, and the BMC's embedded network interfaces.

Host-BMC communication over the same physical LAN connection, also known as "loopback", is not supported. This includes "ping" operations.

2.4.3   IPMI 2.0 Channel Management

Every messaging interface is assigned an IPMI channel ID by IPMI 2.0. Commands are provided to configure each channel for privilege levels and access modes. The following table shows the standard channel assignments.

Table 9. IPMI Channel ID Assignments

Channel ID	Interface		Supports Sessions
	Intel® Server Board S5500BC	Intel® Server Board S5500HC, Intel® Server Board S5520SC, Intel® Server Board S5520UR, Intel® Server Board S5520WB and Intel® Server Board S3420GP	
0	Primary IPMB	Primary IPMB	No
1	LAN 1 (only accessible through NIC_2)	LAN 1 (Switchable between the two on-board NIC ports on the server board)	Yes
2	Reserved (To be used on future products to support 2 LAN channels on the baseboard)	Reserved (To be used on future products to support 2 LAN channels on the server board)	–
3	LAN 2 (Provided by the RMM3 card)	LAN 2 (Provided by the RMM3 card)	Yes
4	Serial (COM2 terminal mode only)	Serial (COM2 terminal mode only)	Yes
5	USB	USB	No
6	Secondary IPMB	Secondary IPMB	No
7	SMM	SMM	No
8 – 0Dh	Reserved	Reserved	–
0Eh	Self	Self	–
0Fh	SMS/Receive Message Queue	SMS/Receive Message Queue	No

2.4.4   BMC IP Address and external connection

The BMC IP address for a particular embedded NIC is always different from the IP address of the Server's operating system.

The BMC supports static and DHCP sourced IP address assignment on all of its management NICs. The IP address source parameter must be set to "static" before the IP address, subnet mask, or gateway address can be manually set.

If the BMC's IP address on a LAN channel changes while a LAN session is in progress over that channel, the BMC does not take action to close the session except through a normal session timeout. The remote

client must re-sync with the new IP address.

The BMCs communicate through NIC 1 or NIC 2 depending on your network configuration. To communicate with the BMC, you need to attach a standard Ethernet cable. You can use PING to confirm that this connection is valid.

For details on which Ethernet port is shared with the BMC to ensure successful communication, see the following table.

Table 10. Shared Ethernet ports with BMC

Intel® Server Boards	System Ethernet port shared with the BMC
Intel® Server Board S5500BC	On-board NIC 2 only
Intel® Server Board S5500HC	On-board NIC 1 only
Intel® Server Board S5520SC	On-board NIC 1 only
Intel® Server Board S5520UR	On-board NIC 1 only
Intel® Server Board S3420GP	On-board NIC 1 only (Note: V SKU don't have BMC)

The following figure displays the location for NIC1 and NIC2 on Intel® Server System SR2600UR to serve as a reference.

✎ **NOTE**

The location of the on-board NICs may be slightly different on other Intel® server boards.


A	On-board NIC2
B	On-board NIC1

Figure 6. Rear connectors of the Intel® Server System SR2600UR

2.4.5　Secure Shell (SSH)

Secure Shell (SSH) connections are supported for SMASH-CLP sessions to the BMC.

2.4.6   BMC Users

The BMC supports the IPMI 2.0 user model including support for *User ID 1*. 15 user IDs are supported. These 15 users can be assigned to any channel. The following restrictions are placed on user-related operations:

- User names for User IDs 1 and 2 cannot be changed. These will always be "" (Null) and "root" respectively.

- User 2 ("root") will always have the administrator privilege level.

- All user passwords (including passwords for 1 and 2) may be modified.

- User IDs 3-15 may be used freely, with the condition that user names are unique. Therefore, no other users can be named as "" (Null), "root," or any other existing user name.

Table 11. Feature Comparison

Users	User Name	Password	Status	Characteristics
User 1	Null	Null	Disabled	Only Password can be changed.
User 2	root	superuser	Disabled	Only Password can be changed.
User 3	test1	superuser	Disabled	Both user name and password can be changed.
User 4	test2	superuser	Disabled	Both user name and password can be changed.
User 5	test3	superuser	Disabled	Both user name and password can be changed.
User 6-15	undefined	undefined	Disabled	Both user name and password can be changed.

Intel® recommends changing the password if using user 1 or 2, and changing both user name and password if using user 3-5.

2.4.7   Session Support

Maximum/Minimum session support varies by interface type:

- IPMI Over LAN – Maximum of five sessions

- Embedded WebServer (when advanced features are enabled) – Minimum of four sessions

- Media Redirection – Minimum of two sessions

- KVM – Minimum of two sessions

- Serial Channel – One session only

2.4.8   Intel® Remote Management Module 3 (RMM3)

The Intel® RMM3 provides the integrated BMC with an additional dedicated network interface. The dedicated interface consumes its own LAN channel. Intel® RMM3 supports advanced features such as KVM redirection and Media redirection.

Intel® RMM2 uses its own user authorization, while Intel® RMM3 uses BMC's user authorization.

Intel® RMM2 uses its dedicated utility, Psetup.exe, to configure Intel® RMM2's IP address, user name, and password. Intel® RMM3 uses common utilities, such as the Intel® Deployment Assistant (IDA), SYSCFG utility or BIOS menu to configure its IP address, username, and password for remote access.

The web server is available on all enabled LAN channels. If a LAN channel is enabled, properly configured, and accessible, the web server is available.

For security reasons, the null user (user 1) may not be used to access the web server. The session inactivity timeout for the embedded web server is 30 minutes. This is not user-configurable.

Basically, you can easily configure Intel® RMM3 for remote access using IDA or SYSCFG:

- Set user's password (other than anonymous users)
- Enable that user on BMC LAN Channel 3 (for Intel® RMM3)
- Configure BMC LAN Channel 3's IP address (DHCP or static IP)

For detailed information on how to configure and use Intel® RMM3, refer to the *Intel® Remote Management Module 3 User Guide*.

2.4.9 Access BMC through Intel® RMM3

The Intel® RMM3 is IPMI V2.0 Compliant. It allows the customer to remote access BMC through Intel® RMM3's dedicated LAN channel (LAN channel 3).

- The customer can send IPMI commands through the dedicated NIC on the Intel® RMM3.
- Intel® RMM3 also supports SOL over this channel. The customer can activate SOL session through the dedicated NIC on the Intel® RMM3.
- In order to access BMC through Intel® RMM3, you must configure Intel® RMM3's IP address and associate BMC user ID to BMC LAN channel 3.

2.5 BMC in Intel Server S1200BT Series Boards

2.5.1 LAN interface

Intel® S1200BT Server boards (BMC SKU) series embedded with the Integrated BMC. The Integrated BMC implements both the IPMI 1.5 and IPMI 2.0 messaging models. These provide out-of-band local area network (LAN) communication between BMC and external network.

2.5.2 BMC Embedded LAN Channels

BMC hardware includes three dedicated network interfaces:

- **Interface 1:** This interface is available from the 1st on-board NIC ports in a system, which can be shared with the host. Only one NIC may be enabled for management traffic at any time.
- **Interface 3:** This interface is available from an optional Intel® RMM4, which is a dedicated

management NIC and not shared with the host.

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

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

- IP Address: Static

- All users disabled

IPMI-enabled network interfaces may not be placed on the same subnet. This includes the Intel® RMM4's on-board network interface, and the BMC's embedded network interfaces.

Host-BMC communication over the same physical LAN connection, also known as "loopback", is not supported. This includes "ping" operations.

2.5.3   Dedicated MAC Address

Each of the BMC's two NIC channels has a unicast MAC filter reserved for BMC use. These filters enable the BMC to receive network data streams that are logically separate from, and invisible to, operating systems and software running on the server, despite sharing the same physical LAN connections. This allows the BMC to support features beyond standard IPMI-over-LAN, such as DHCP, full ARP request/response, and ICMP, without requiring a separate Ethernet cable.

For Intel® S1200BT series server boards, each server board has four MAC addresses assigned to it at the Intel factory. The printed MAC address is assigned to NIC1 on the server board.

- NIC 1 MAC address (for OS usage)

- NIC 2 MAC address = NIC 1 MAC address + 1 (for OS usage)

- BMC LAN channel 1 MAC address = NIC1 MAC address + 2

- BMC LAN channel 3 MAC address = NIC2 MAC address + 2

2.5.4   IPMI 2.0 Channel Management

Every messaging interface is assigned an IPMI channel ID by IPMI 2.0. Commands are provided to configure each channel for privilege levels and access modes. The following table shows the standard channel assignments.

Table 12. IPMI Channel ID Assignments

Channel ID	Interface	Supports Sessions
0	Primary IPMB	No
1	LAN 1 (only accessible by means of 82574L LAN port, NIC_2)	Yes
2	Reserved (To be used on future products to support 2 LAN channels on the baseboard)	–
3	LAN2 [1] (Provided by the Intel® Dedicated Management NIC)	Yes

Channel ID	Interface	Supports Sessions
4	Reserved	Yes
5	USB	No
6	Secondary IPMB	No
7	SMM	No
8 – 0Dh	Reserved	–
0Eh	Self [2]	–
0Fh	SMS/Receive Message Queue	No

2.5.5 BMC IP Address and external connection

The BMC IP address for a particular embedded NIC is always different from the IP address of the Server's operating system.

The BMC supports static and DHCP sourced IP address assignment on all of its management NICs. The IP address source parameter must be set to "static" before the IP address, subnet mask, or gateway address can be manually set.

If the BMC's IP address on a LAN channel changes while a LAN session is in progress over that channel, the BMC does not take action to close the session except through a normal session timeout. The remote client must re-sync with the new IP address.

To communicate with the BMC, you need to attach a standard Ethernet cable to NIC 1. You can use PING to confirm that this connection is valid.

The following figure displays the location for NIC1 and NIC2 on Intel® Server System S1200BT to serve as a reference.

✏ **NOTE**

The location of the on-board NICs may be slightly different on other Intel® Server Boards.
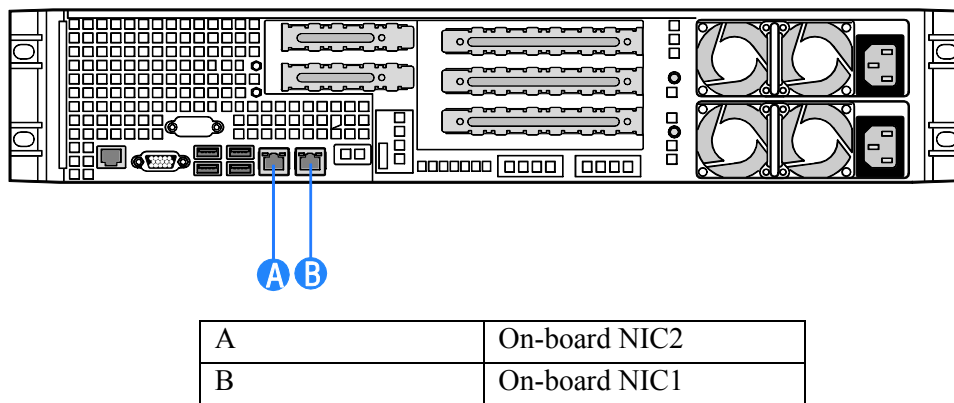

D	On-board NIC1
E	On-board NIC2
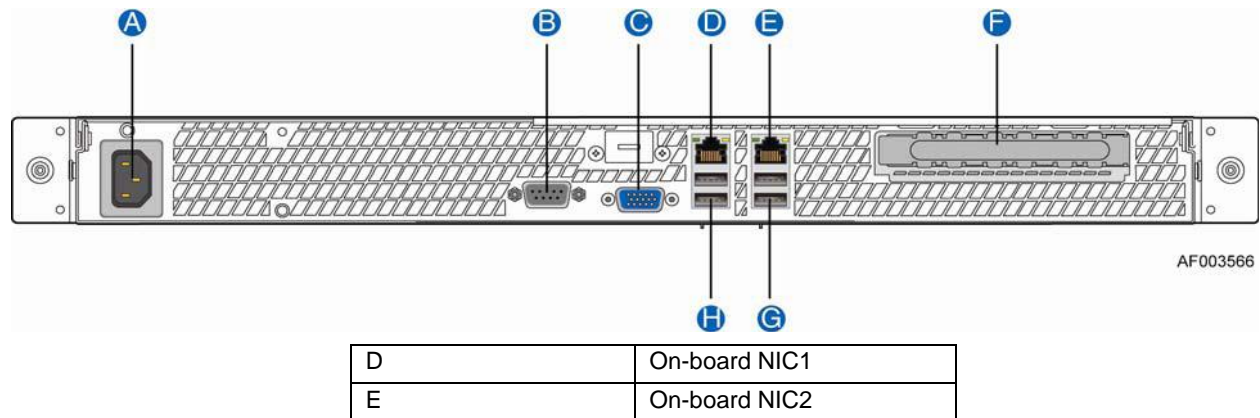
Figure 7. Rear connectors of the Intel® Server System R1304BT

2.5.6 Secure Shell (SSH)

Secure Shell (SSH) connections are support for SMASH-CLP sessions to the BMC.

2.5.7 BMC Users

The BMC supports the IPMI 2.0 user model including support for *User ID 1*. 15 user IDs are supported. These 15 users can be assigned to any channel. The following restrictions are placed on user-related operations:

- User names for User IDs 1 and 2 cannot be changed. These will always be "" (Null) and "root" respectively.

- User 2 ("root") will always have the administrator privilege level.

- All user passwords (including passwords for 1 and 2) may be modified.

- User IDs 3-15 may be used freely, with the condition that user names are unique. Therefore, no other users can be named as "" (Null), "root," or any other existing user name.

Table 13. Feature Comparison

Users	User Name	Password	Status	Characteristics
User 1	Null	Null	Disabled	Only Password can be changed.
User 2	root	superuser	Disabled	Only Password can be changed.
User 3	test1	superuser	Disabled	Both user name and password can be changed.
User 4	test2	superuser	Disabled	Both user name and password can be changed.
User 5	test3	superuser	Disabled	Both user name and password can be changed.
User 6-15	undefined	undefined	Disabled	Both user name and password can be changed.

Intel recommends changing the password if using user 1 or 2, and changing both user name and password if using user 3-5.

2.5.8 Session Support

Maximum/Minimum session support varies by interface type:

- IPMI Over LAN – Maximum of 4 sessions

- Embedded Web Server (with or without Intel® RMM4 installed) – Minimum of two sessions

- Media Redirection – Minimum of two sessions

- KVM – Minimum of two sessions

- Serial Channel – One session only

2.5.9   New Features of BMC

Comparing with Intel® S5500 series server boards, in this generation of Servers, we added some new features to BMC (Even no Intel® RMM4 module installed), there are:

- **Embedded Web Server**

BMC Base manageability provides an embedded web server and an OEM-customizable web GUI which 个 exposes the manageability features of the BMC base feature set. It is supported over all on-board NICs that have management connectivity to the BMC as well as an optional dedicated add-in management NIC. At least two concurrent web sessions from up to two different users is supported.

Figure 8. System Information Window

The GUI presented by the embedded web server authenticates the user before allowing a web session to be initiated. It presents all functions to all users but grays-out those functions that the user does not have privilege to execute. (e.g. if a user does not have privilege to power control, then the item shall be displayed in grey-out font in that user's UI display). The web GUI also provides a launch point for some of the advanced features, such as KVM and media redirection. These features are grayed out in the GUI unless the system has been updated to support these advanced features.
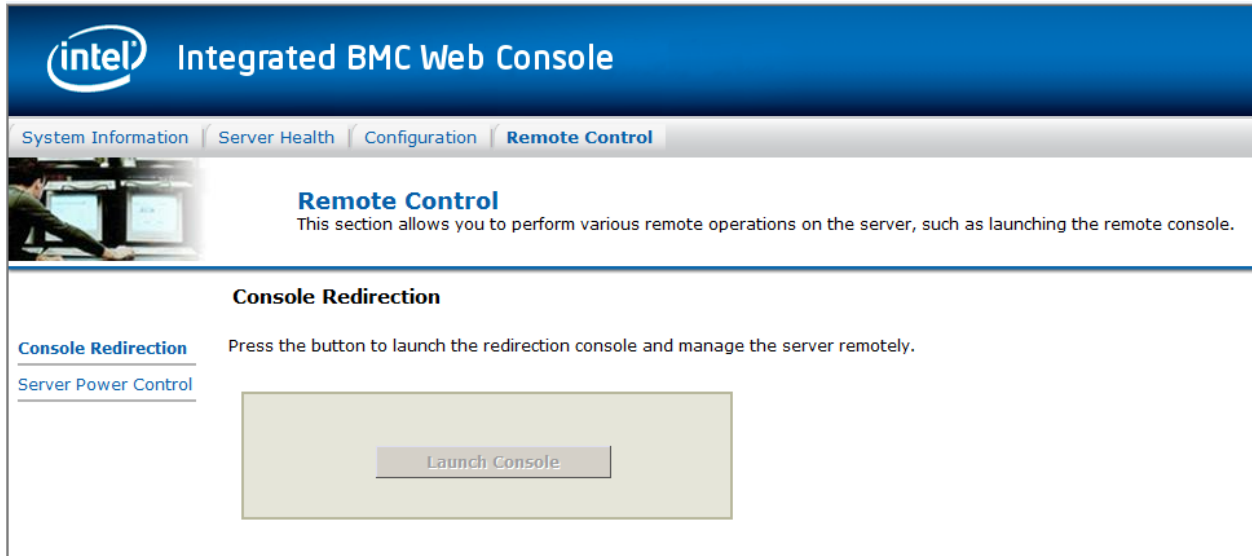
Figure 9. Console Redirection Window

Additional features supported by the web GUI includes:
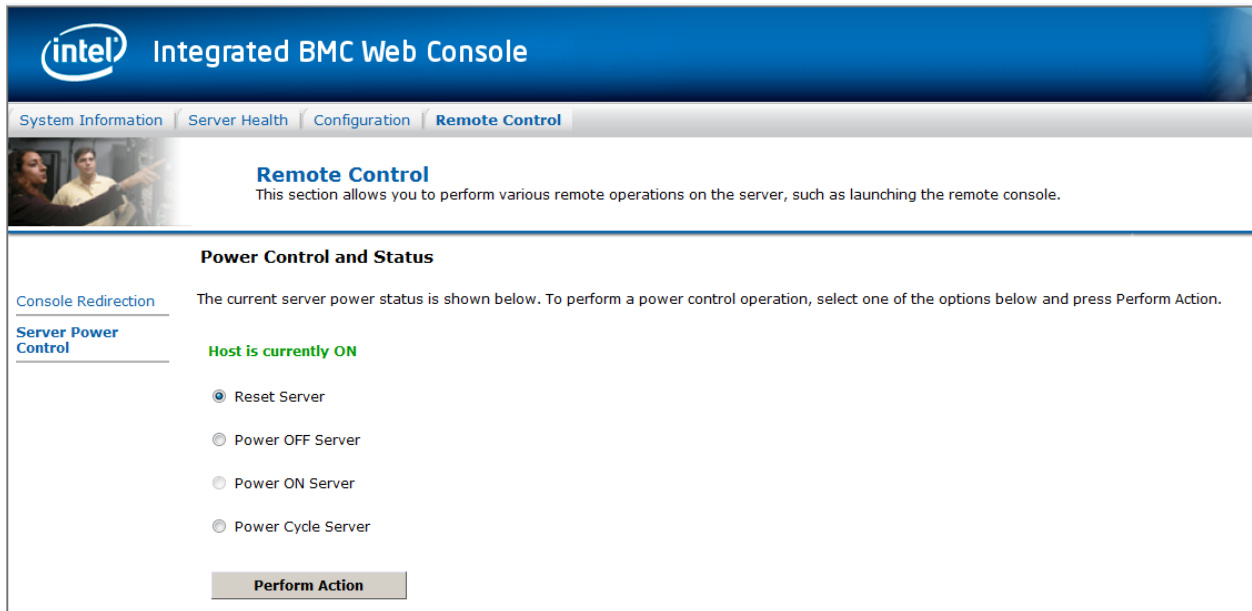
Figure 10. Power Control and Status Window

- Presents all the Basic features to the users.
- Power on/off/reset the server and view current power state.
- Displays BMC, ME and SDR version information.
- Display overall system health.
- Configuration of various IPMI over LAN parameters for both IPV4
- Configuration of alerting (SNMP and SMTP).

- − Display system asset information for the product, board, and chassis.

- Display of BMC-owned sensors (name, status, current reading, enabled thresholds), including color-code status of sensors. P

- Provides ability to filter sensors based on sensor type (Voltage, Temperature, Fan & Power supply related)

- Automatic refresh of sensor data with a configurable refresh rate.

- On-line help.

- Display/clear SEL (display is in easily understandable human readable format).

- Supports major industry-standard browsers (Microsoft Internet Explorer* and Mozilla Firefox*).

- Automatically logs out after user-configurable inactivity period.

- Embedded Platform Debug feature - Allow the user to initiate a "diagnostic dump" to a file that can be sent to Intel for debug purposes.

- Severity level indication of SEL events. The web server UI displays the severity level associated with each event in the SEL. The severity level correlates with the front panel system status LED ("OK", "Degraded", "Non-Fatal", or "Fatal").

- Display of memory information as is available over IPMI over LAN.

- Ability to view and configure VLAN settings.

- Capability to block logins for a period of time after several consecutive failed login attempts. The lock-out period and the number of failed logins that initiates the lock-out period are configurable by the user.

- **Embedded Platform Debug**

The Embedded Platform Debug feature supports capturing low-level diagnostic data (applicable MSRs, PCI config-space registers, etc.). This feature allows a user to export this data into a file that is retrievable through the embedded web GUI, as well as through host and remote IPMI methods, for the purpose of sending to an Intel engineer for an enhanced debugging capability. The files are compressed, encrypted, and password protected. The file is not meant to be viewable by the end user but rather to provide additional debugging capability to an Intel support engineer.

A list of data that may be captured using this feature includes but is not limited to:

- Platform sensor readings

  – This includes all "readable" sensors that can be accessed by the BMC FW and have associated SDRs populated in the SDR repository. This does not include any "event-only" sensors. (All BIOS sensors and some BMC and ME sensors are "event-only"; meaning that they are not readable using an IPMI Get Sensor Reading command but rather are used just for event logging purposes).

- SEL

  – The current SEL contents are saved in both hexadecimal and text format.

- CPU/memory register data useful for diagnosing the cause of the following system errors: CATERR, ERR[2], SMI timeout, PERR, and SERR

   - The debug data is saved and timestamped for the last 3 occurrences of the error conditions.

      a. PCI error registers

      b. MSR registers

      c. MCH registers

- BMC configuration data

- BMC FW debug log (that is, SysLog)

   – Captures FW debug messages.

      ◈ SMBIOS table data. The entire SMBIOS table is captured from the current boot.

      ◈ PCI configuration data for on-board devices and add-in cards. The first 256 bytes of PCI configuration data is captured for each device for each boot.

      ◈ System memory map. The system memory map is provided by BIOS on the current boot. This includes the EFI memory map and the Legacy (E820) memory map depending on the current boot.

- **Data Center Management Interface (DCMI)**

The DCMI Specification is an emerging standard that is targeted to provide a simplified management interface for Internet Portal Data Center (IPDC) customers. It is expected to become a requirement for server platforms which are targeted for IPDCs. DCMI is an IPMI-based standard that builds upon a set of required IPMI standard commands by adding a set of DCMI-specific IPMI OEM commands.

- **Lightweight Directory Authentication Protocol (LDAP)**

The Lightweight Directory Access Protocol (LDAP) is an application protocol supported by the BMC for the purpose of authentication and authorization. The BMC user connects with an LDAP server for login authentication. This is only supported for non-IPMI logins including the embedded web UI and SM-CLP. IPMI users/passwords and sessions are not supported over LDAP.

LDAP can be configured (IP address of LDAP server, port, etc.) through the BMC's Embedded Web UI. LDAP authentication and authorization is supported over the any NIC configured for system management. The BMC uses a standard Open LDAP implementation for Linux*. Only open LDAP is supported by BMC. Windows* and Novell* LDAP are not supported.

2.5.10   Intel® Remote Management Module 4

The Intel® RMM4 works as an integrated solution on your server system. Based on an embedded operating system, the Intel® RMM4 add-on card provides both exceptional stability and permanent availability independent of the present state of the server's operating system. As a system administrator, you can use the Intel® RMM4 to gain location-independent remote access to respond to critical incidents

and to undertake necessary maintenance.

Intel® RMM4 is comprised of up to two boards – Intel® RMM4 Lite and the optional Intel® Dedicated Server Management NIC (DMN).

Figure 11. Intel® RMM4 Lite and Dedicated NIC

The Intel® RMM4 Lite is a small board that unlocks advanced management features on the RGMII 1Gb interface when installed on Intel® server boards. It provides an increased level of manageability over the basic server management available to the server board. It works as an integrated solution on your server system. If the optional Dedicated Server Management NIC is not used then the traffic can go through the onboard Integrated BMC-shared NIC and share network bandwidth with the host system.

The Intel® RMM4 add-on offers convenient, remote KVM access and control through LAN or Internet. It captures, digitizes, and compresses video and transmits it with keyboard and mouse signals to and from a remote computer. Remote access and control software runs in the Integrated Baseboard Management Controller, utilizing expanded capabilities enabled by the Intel® RMM4 hardware.

Key features of the Intel® RMM4 add-on card are:

- KVM redirection through either the RMM4 NIC or the baseboard NIC used for management traffic; up to two simultaneous KVM sessions.
- Media redirection – The media redirection feature is intended to allow system administrators or users to mount a remote IDE or USB CD-ROM, floppy drive, or a USB flash disk as a remote device to the server. Once mounted, the remote device appears just like a local device to the server, allowing system administrators or users to install software (including operating systems), copy files, update BIOS, and so on, or boot the server from this device.
- KVM - Automatically senses video resolution for best possible screen capture, high-performance mouse tracking and synchronization. It allows remote viewing and configuration in pre-boot POST and BIOS setup.

Intel® RMM4 uses BMC's user authorization. In order to access Intel® RMM4 or Intel® RMM4 Lite, you have to use common utilities, such as the Intel® Deployment Assistant (IDA), SYSCFG utility or BIOS menu to configure its IP address, username, and password before doing remote access:

- Set user's password (other than anonymous users)

- Enable that user on BMC LAN Channel 3 (for Intel® RMM4)
- Configure BMC LAN Channel 3's IP address (DHCP or static IP)

The web server is available on all enabled LAN channels. If a LAN channel is enabled, properly configured, and accessible, the web server is available.

For security reasons, the null user (user 1) may not be used to access the web server. The session inactivity timeout for the embedded web server is 30 minutes. This is not user-configurable.

For detailed information on how to configure and use Intel® RMM4 and Intel® RMM4 Lite, refer to the *Intel® Remote Management Module 4 User Guide*.

2.5.11   Access BMC through Intel® RMM4

The Intel® RMM4 is IPMI V2.0 Compliant. It allows the customer to remote access BMC through Intel® RMM4's dedicated LAN channel (LAN channel 3).

- The customer can send IPMI commands through the dedicated NIC on the Intel® RMM4.
- Intel® RMM4 also supports SOL over this channel. The customer can activate SOL session through the dedicated NIC on the Intel® RMM4.

In order to access BMC through Intel® RMM4 Lite and RMM4, you must configure Intel® RMM4's IP address and associate BMC user ID to BMC LAN channel 1 or LAN channel 3.

3 BMC Firmware Update Procedure

BMC firmware can be updated from pre-OS and OS present environments, such as Extensible Firmware Interface, Microsoft Windows* Preinstallation Environment (WinPE), Microsoft Windows* Server and Red Hat* or SuSE* Linux Enterprise Server operating systems.

You can download the server firmware update package from http://www.intel.com/support.

3.1 Update BMC firmware under EFI

Intel provides a firmware update package for EFI for each platform on the support web site. In order to download the update and run it under EFI, a USB key is frequently used. Use the following steps for reference:

- Copy "Firmware update package for EFI" (name may vary depending on the platform) to the USB Key and insert USB key to the system.
- Boot system to EFI.
- Change from EFI shell to USB key (for example, **fs0:**).
- Change directory to the folder where the BMC update package is located.
- Run "BMCxx.nsh" to perform the BMC update.
- After update is completed, reboot the system.
- Verify that the BMC firmware has been successfully updated by viewing "System Management Page" in the BIOS menu.

3.2 Update BMC firmware under WinPE

Windows Preinstallation Environment (WinPE):

In order to build a customized WinPE CD for factory build purpose, you have to prepare the following content:

- The package "Firmware Update Package for the Intel® Deployment Assistant, Intel® One-boot Flash Utility, Intel® embedded EFI shell, and Microsoft Windows* Preinstallation Execution Environment (WinPE)" (name of the package may vary depending on the platform) is posted for each platform on Intel's support web site. This download contains BIOS, BMC, FRUSDR, and HSC code for use with the customized WinPE CD.
- Microsoft WinPE* CD
- "BIOS, Firmware Update and Configuration utilities for Windows* PE" for each platform on the support web site.

Detailed instructions for building the Customized WinPE CD are available on Intel's support web site under the "BIOS, Firmware Update and Configuration utilities for Windows* PE" package by clicking

the "Deployment Procedure for Microsoft Windows* Preinstallation Environment" link.

3.3   Update BMC firmware under IDA

Intel® Deployment Assistant:

To use IDA, download and copy "Firmware Update Package for the Intel® Deployment Assistant, Intel® One-boot Flash Utility, Intel® embedded EFI shell and Microsoft Windows* Preinstallation Execution Environment (WinPE)" (name of the package may vary depending on the platform) to your USB key:

- Boot system using the Intel® Server Deployment Toolkit CD that shipped with the system.
- Click "Get System Updates". It will automatically locate and download the latest update packages (BIOS, BMC firmware, and FRUSDR) and choose the updates to be applied to this server.
- Under the "Download Updates" page, select "From USB Disk on Key or hard disk" and browse the "Firmware Update Package for the Intel® Deployment Assistant, Intel® One-boot Flash Utility, Intel® embedded EFI shell and Microsoft Windows* Pre-Boot Execution Environment (WinPE)" zip file (file name may vary depending on the platform).
- After FW update is completed, reboot the system.

3.4   Update BMC firmware using OFU for Windows

Microsoft Windows*:

This method requires the Intel® One Boot Flash Update utility (Intel® OFU), which needs to be downloaded from Intel's support web site and is part of the "BIOS, Firmware Update and configuration utilities for Windows*":

- Extract the Intel® OFU package for Microsoft Windows* and double-click Setup_Win.exe. It will install the Intel® OFU utility for Microsoft Windows* to your system. You can also use the Intel® System Management Software CD to install the Intel® OFU utility from the CD's auto-run menu.
- Download and copy "Firmware Update Package for the Intel® Deployment Assistant, Intel® One-boot Flash Utility, Intel® embedded EFI shell and Microsoft Windows* Preboot Execution Environment (WinPE)" (name may vary depending on the platform) from the support web site to your USB key.
- Run flashupdt –u /updatepackage_location

The new BMC firmware takes effect the next time system is rebooted.

3.5   Update BMC firmware using OFU for Linux*

Linux*:

Intel provides a solution to allow the customer to update the BMC firmware while Linux* OS is running.

This method requires the Intel® One Boot Flash Update Utility (Intel® OFU), which needs to be downloaded from Intel's support web site and is part of the "BIOS, Firmware Update and configuration

utilities for Linux*".

- Extract the Intel® OFU package for Linux* and run ./setup to install the Intel® OFU utility on your system.

- Download and copy "Firmware Update Package for the Intel® Deployment Assistant, Intel® One-boot Flash Utility, Intel® embedded EFI shell and Microsoft Windows* Preboot Execution Environment (WinPE)" (name may vary depending on the platform) from the support web site to your USB key.

- Run flashupdt –u /updatepackage_location

The new BMC firmware takes effect the next time system is rebooted.

✏ **NOTE**

The Intel® OFU utility is case sensitive. Therefore, when you transfer the Firmware Update Package using USB key from a Microsoft Windows* system to a Linux* environment, you must first extract under the Microsoft Windows* environment. Otherwise, you will need to mount the USB key manually with "vfat" option under Linux* to avoid conversion from upper case to lower case and vice versa.

4 Server Management Software and Utilities

In order to perform in-band and out-of-band management of Intel® Servers, Intel provides several solutions such as tools, utilities, and management software to allow you to manage the system easily.

This chapter provides an overview of Intel® Server management utilities, tools,and software.

4.1 SYSCFG Utility

The Intel® System Configuration Utility (SYSCFG) is a command-line utility that can be used to save and restore BIOS and BMC firmware settings to a file or to set and display individual settings.

SYSCFG is a command-line, scriptable utility. It can be used in a script to automate the process of configuring multiple servers.

The general syntax is: syscfg <switch> <argument1> <argument2> ...

Example: # syscfg /sole 1 enable 1 19200 6 50

For detailed information, refer to the *SYSCFG User Guide* that is provided with BIOS, Firmware Update, and Configuration Utilities under http://www.intel.com/.

4.1.1 Supported Operating Systems

SYSCFG can be run from pre-OS boot and post-OS boot environments:

- Extensible Firmware Interface (EFI)
- Microsoft Windows* Installation Environment
- Microsoft Windows*
- Linux*

Some platforms may not support all the operating environments for this utility. Refer to the *SYSCFG User Guide* for details.

4.1.2 SYSCFG INI file

From Intel® S5500 Server boards, the utility supports saving and restoring BIOS and firmware settings both in binary and text mode (from a text file, known as INI file). The advantage of using an INI file is that you can modify and change the values of any of the settings available in the INI file.

To save the BIOS and firmware configuration to an INI file, do the following:

- Boot to one of the supported operating systems on the target system.
- Change directories to the location of the syscfg executable. (This location must be writable to allow

you to save the system configuration.)

   – In Microsoft Windows*, Windows Preinstallation Environment*, or EFI, type: `syscfg /s ini filename.ini`

   – In Linux*, type: `./syscfg /s ini filename.ini`

If you have already saved the configuration to a file, use the following procedure to restore the system to the saved configuration, or set the configuration on identical servers to the saved configuration.

Unlike restoring from a binary file, the advantage of using an INI file is that you can modify and change the values of any of the settings available in the INI file. In this scenario, the INI file does not clone servers but provides a mechanism of configuring the same items with different values per your requirement.

✏ **NOTE**

For restoring uneditable fields, section name headers and key names should not be edited or deleted from the INI file.

To restore a configuration with the settings defined in an INI file, do the following:

- Boot the system to one of the supported operating systems.

- Change directories to the directory containing the syscfg executable. (The saved configuration file should also be located in this directory.)

   – In Microsoft Windows*, Windows Preinstallation Environment*, or EFI, type: `syscfg /r ini filename.ini /b`

   – In Linux*, type: `./syscfg /r ini filename.ini /b`

4.1.3   SYSCFG installation and usage

- Linux*:

   – Download BIOS, Firmware Update, and Configuration Utilities for Linux* from http://www.intel.com/ and unzip the "syscfg-linux.zip" file into a folder on your Linux* system.

   – Run the 'installme' script to install the 'syscfg' and 'smi' rpms.

   The SYSCFG utility is installed in the path /usr/local/syscfg.

- UEFI

   – Set the syscfg path variable SYSCFG_PATH.

      Example: - set SYSCFG_PATH fs0:\<syscfg_efi>

      where syscfg_efi is the folder containing all the files mentioned above.

   – Run 'syscfg' commands from the location where the files are copied.

- Windows

- − Download BIOS, Firmware Update, and Configuration Utilities for Linux* from http://www.intel.com/.
  - ▪ For 32-bit platforms, go to the InstallationIA32 folder from the command prompt, and run Install.Cmd.
  - ▪ For EM64T platforms, go to the InstallationEM64T folder from the command prompt, and run Install.Cmd.

The above command will install the respective drivers to be used by the SysCfg utility.

- − From the command prompt, go to SysCfg Release folder and run the desired commands for the utility.

- WinPE

For information about customizing your own WinPE CD image, refer to the white paper available on the support web site under the "BIOS, Firmware Update and Configuration utilities for Windows* PE" package.

4.2   Intel® Deployment Assistant CD

The Intel® Deployment Assistant (IDA) provides a single interface with an easy to use HTML like graphic UI to ease the process of setting up and deploying an Intel server from initial boot through the initiation of an unattended OS installation.

Each Intel® server board ships with a copy of Intel® Deployment Assistant CD.

Intel® Deployment Assistant helps a system administrator do the following:

- Update an Intel® server with the latest system software. Updates can be got from a set URL (http://www.intel.com/support which can be customized by OEM), a network drive, or removable media. The firmware components that can be updated using Intel® Deployment Assistant are: BIOS, Integrated BMC (iBMC), non expander HSCs, and SDRs.
- Configure the most common options of the BIOS and firmware.
- Configure a RAID volume on attached hard drives
- Install Windows* and Linux* operating systems
- Clone all deployment work from one server to multi server

✎   NOTE

The installation is fully unattended *except* for a license screen agreement that you can agree to *and* any changing of CDs.

The latest drivers for all the on-board components are added from IDA CD or from other supported locations during the OS installation

Intel® Deployment Assistant is a browser based graphical application that provides an easy to use, wizard style interface to the system administrator for performing all the above tasks. It is packaged onto a single CD which contains its own operating system (Linux*), a GUI, Intel® Deployment Assistant core, and

supporting files for setup and deployment. Intel® Deployment Assistant boots automatically from a CD-ROM/USB drive and runs completely in a RAMDISK.

Figure 12. Intel® Deployment Assistant CD Homepage

4.2.1   Get System Updates

A system firmware update can be performed in an online or offline manner.
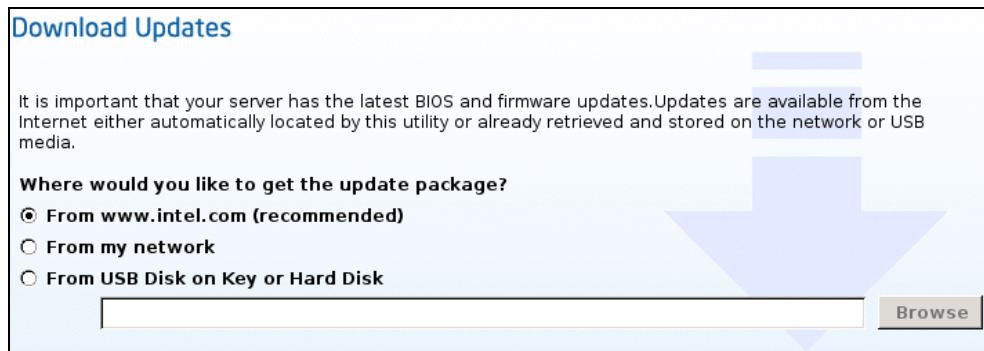
Figure 13. System Update page of IDA CD

Optionally, the user can:

- Perform online update from http://www.intel.com/
- IDA can automatically mount the remote network drive using the user name, password and remote

network share name provided by the user

- IDA can automatically detect USB disk on key devices; therefore, packages can be downloaded and stored on USB disk on key devices

4.2.2 Configure a server

IDA allows the user to configure key BIOS and server management settings. A wizard automatically displays only the screens that the user chooses to configure on the server, for example, set the asset tag, configure BIOS, and configure server management such as set the BMC LAN channel information.

Figure 14. Configure a server page on the IDA CD

4.2.3 RAID configuration

It can be hard for users to keep track of the differences between the various RAID controllers used with Intel's platforms. IDA provides simplified, easy to understand configuration options that are common across all (or most) Intel® RAID controllers so that underlying differences are not exposed.

RAID Configuration depends on the number of disks found connected. User is provided with any of these 3 options:

- Auto with redundancy
- Auto Without redundancy
- Custom configuration

Also, RAID levels, stripe size, Logical volume size and other details can be selected as appropriate.

The RAID Configuration function helps an OS installation to a RAID logical volume when the user chooses the option.
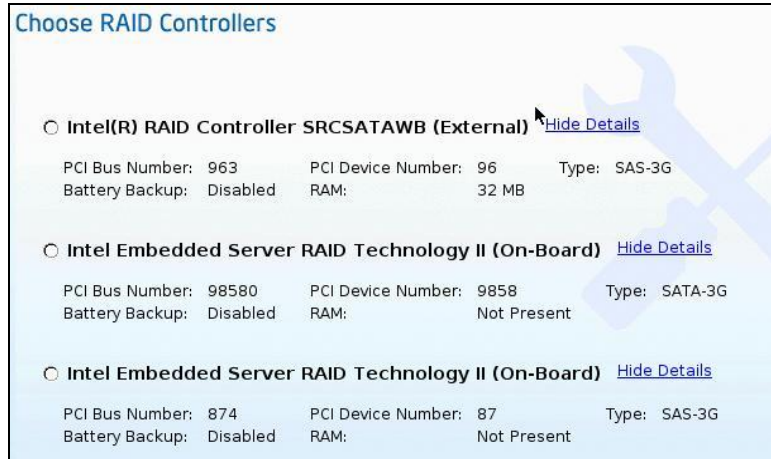
Figure 15. RAID Controllers Selection Page

4.2.4   Unattended OS installation

IDA can be used to configure an unattended OS installation, resulting in the user answering questions within the IDA user interface and then adding the OS CD(s). OS installation starts automatically after the server reboots and requires no further input.

Supported Operating Systems:

- Microsoft Windows*
- Linux* (SuSE* and Red Hat* Enterprise Linux)
- VMware
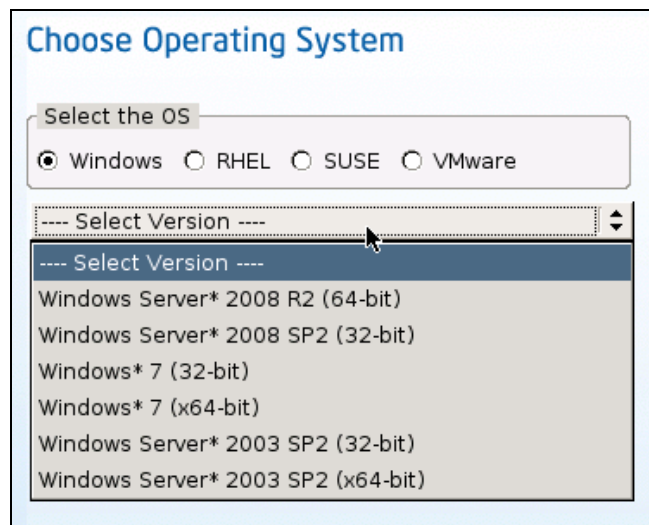
Figure 16. Unattended Installation GUI screen

4.3   Intel® SEL Viewer

The Intel® System Event Log (SEL) Viewer is used to display, clear, or save the SEL on your server.

The Baseboard Management Controller (BMC) records details about the system events in a log in flash memory. Each SEL entry is a single system event.

The SEL Viewer utility provides the ability to view system event records stored on the server management storage device of a server. The utility displays the SEL records in either a text or hexadecimal format. The utility also allows the user to save SEL entries to a file and load SEL entries from a file for viewing. The user can also reload SEL entries from a server and see properties of SEL entries. The SEL entries can be viewed in two modes: interpreted text mode and hex mode.

The SEL Viewer utility runs on the target servers in:

- Extensible Firmware Interface (EFI) shell
- Microsoft Windows Preboot Environment* command window
- Microsoft Windows Server 2003* SP1 and Windows XP* SP2)
- Linux*

4.3.1   The SEL Log format

The SEL entry is originally in HEX format. The SEL viewer utility has the ability to translate the SEL records from hexadecimal format to human readable text format.

Example:

HEX format SEL entry:

RID:[04][00] RT:[02] TS:[2F][58][71][48] GID:[20][00] ER:[04] ST:[10] SN:[09] EDIR:[6F] ED1: [42] ED2: [0F] ED3: [FF]

Corresponding text SEL entry:

07/06/2008-23:41:35   Event Log Cleared /System Event Log   The BMC on S5400SF has reported an informational assertion event for System Event Log. The event has the following information: the log area has been reset and/or cleared. There is no recommended action defined for this event.   BMC - LUN #0 (Channel #00h)

4.3.2   Launching the Intel® SEL Viewer

The SEL Viewer utility can be run from the command line or GUI interface depending on the OS that is running:

- Command line:

    selview [**/clear** | {**/save** [*filename*] [**/hex**]} | **/h** | **/?**]

- Launch SEL viewer in GUI interface mode:

Figure 17. SEL Viewer GUI page for Linux*

For detailed information on how to use the SEL viewer, refer to the *System Event Log (SEL) Viewer Utility User Guide* that is provided with BIOS, Firmware Update, and Configuration Utilities.

4.4 Intel® System Information Retrieve Utility

The Intel® System Information Retrieval Utility (hereinafter referred to as sysinfo) is used for collecting system information.

Intel offered UEFI version, Windows version and Linux* version Intel® System Information Retrieval Utility that the customers are able to collecting system information under these environments.

4.4.1 Overview

The System Information Retrieval UTILITY (sysinfo) used for collecting the system information. This utility dumps the following information to log files:

1. Platform Firmware Inventory

2. Sensor information

3. Sensor Data Records

4. BMC SEL (IN HUMAN READABLE FORM)

5. BMC SEL (IN HEX FORM)

6. Base Board FRU

7. System BMC Boot Order

8. BMC User Settings

9. BMC LAN Channel Settings

10. BMC SOL Channel Settings

11. BMC Power Restore Policy Settings

12. BMC channel settings

13. SMBIOS Type 1, Type 2, Type 3

14. Processor

15. Memory

16. Operating System Information

17. List of device drivers installed

18. List of s/w installed

19. BIOS Settings (per BIOS SETUP F2 Screen).

20. PCI Bus Device Information

21. RAID settings and RAID log

22. OS event log.

4.4.2   Supported Operating System

Intel offered UEFI version, Windows version and Linux* version Intel® System Information Retrieval Utility that the customers are able to run it and collect system information under these environments.

4.4.3   Install/uninstall

For sysinfo install and uninstall under Windows*/Linux*, you have to refer *Release Notes* and *User Guide* to perform some pre-request tasks. Both sysinfo *User Guide* and *Release Notes* are comes with "BIOS, Firmware Update & Configuration Utilities Package".

```
[root@localhost SysInfo_Linux_V1.0]# cd Linux/
[root@localhost Linux]# ls
install.sh  RHEL  SLES  uninstall.sh

[root@localhost Linux]# source install.sh
dos2unix: converting file rhel-install.sh to UNIX format ...
Intel (R) System Information Retrieval Utility Version 1.0 Build 1
Copyright (c) 2010 Intel Corporation

Preparing...              ######################################## [100%]
Installing....
   1:Lib_Utils2            ######################################## [100%]
Preparing...              ######################################## [100%]
Installing....
   1:Lib_Utils             ######################################## [100%]
Preparing...              ######################################## [100%]
   1:CmdTool2              ######################################## [100%]

dos2unix: converting file backend1.sh to UNIX format ...
dos2unix: converting file backend2.sh to UNIX format ...
dos2unix: converting file backend3.sh to UNIX format ...
dos2unix: converting file backend4.sh to UNIX format ...
dos2unix: converting file backend5.sh to UNIX format ...
dos2unix: converting file rhel-install.sh to UNIX format ...
dos2unix: converting file rhel-uninstall.sh to UNIX format ...

Installation successful.
[root@localhost RHEL]#
```

Figure 18. Sysinfo Installation

4.4.4   Sysinfo logs

Sysinfo log displayed as text log, you can find/search required information from txt results for troubleshooting purpose.

```
-------------------------------------------
System FRU
-------------------------------------------
Displaying Chassis Area

Chassis Information Area (Version 1,Length 112)

ChassisType               : Rack Mount Chassis
Part Number (ASCII)       : 12345678901234567890
Serial Number (ASCII)     : Field not present
Additional Field (ASCII)  : 555
Additional Field (ASCII)  : 555

Displaying Board Area

Unicode Country Base      : 00h
Manufacturing Time(mins)  : 01/01/1970-00:00:00
Manufacturing Name(ASCII) : Intel Corporation
Product Name(ASCII)       : S5520UR
Serial Number(ASCII)      : BNUB84000181
Part Number(ASCII)        : E22554-402
Mftr FRU File ID(ASCII)   : FRU Ver 0.03

Displaying Product Area

Product Information Area (Version 1,Length 104)

Unicode Country Base      : 00h
Manufacturer Name(ASCII)  : Intel
Product Name(ASCII)       : Urbana
Product Version(ASCII)    : ....................
Part Number(ASCII)        : 550004200
Serial Number ID(ASCII)   : 67
Asset Tag(ASCII)          : Field not present
```

Figure 19. Example of part of Sysinfo Log

4.5   Intel® System Management Software

Intel® System Management Software (SMS) offers remote monitoring, configuration, software distribution, updates, and troubleshooting management features. It includes a collection of software applications targeted for all market segments.

Intel® SMS DVD that is shipped with Intel® Server Boards contains the following components:

Table 14. Intel® SMS components

Features	Benefits
Intel® Multi-Server Manager	An easy-to-use web-application that allows users to discover and manage multiple Servers in their network from a single console. It can manage any Server hardware that is IPMI compatible.
Intel® Active System Console	Simple lightweight management console application for server health monitoring.
Intel® Management Packs for use with Microsoft System Center Essentials*	Hardware management packs for Intel® Server Boards, Intel® Modular Server, Intel® vPro or Intel® Centrino® with vPro desktops and laptops. Management Packs integrate seamlessly into Microsoft System Center Essentials 2007* SP1.
Intel® Command Line Interface	Manage Intel® Server Boards using a command line interface that allows users control regardless of the state of the operating system.
Intel® SNMP Subagent	Integrate into an enterprise console that supports SNMP.

For detailed information, please refer to *Intel® System Management Software User Guide* or *Intel® Server Management Pack User Guide* that were included in the Intel® SMS DVD.

The following table lists the features and benefits of Intel® System Management Software Suite of Products:

Table 15. Intel® SMS components

Features	Intel® Multi-Server Manager	Intel® Active System Console	Intel Management packs for the Microsoft System Center*	Intel® SNMP-SA	Intel® Command Line Interface (CLI)
Server Environment	1-100 servers	1-10 servers	10-50 servers (Use Operations Manager for Enterprise)	Enterprise	Any
User Interface	Web Based	Web Based	Windows Management Application	Integrates into enterprise tools such as HP* OpenView	Command Line
Operating System Support	Windows, Linux	Windows, Linux	Windows, Linux	Windows, Linux	Windows, Linux
Single, easy to use console	X	X	X		

Features	Intel® Multi-Server Manager	Intel® Active System Console	Intel Management packs for the Microsoft System Center*	Intel® SNMP-SA	Intel® Command Line Interface (CLI)
Hardware Predictive Failure Analysis	X	X	X	X	X
Sensor readings	X	X	X	X	X
Hardware Event Log	X	X	X		X
Hardware and Software Inventory	X (Hardware and Operating System)	X (Hardware and Operating System)	X		
OS and Application Monitoring			X		
Software Patch Deployment			X		
Application Deployment			X		
Alerting	X (Email or BMC SNMP)	X (Email and BMC SNMP)	X (Email, SNMP, SMS)	X (SNMP)	
Reporting	X	X	X (80 powerful software and hardware reports)		
BMC Configuration	X	X	X		X
Power Management	X	X	X		
Performance Views			X		
Remote Management	X	X	X	X	X
Multi Server Management	X		X		
Remote Power On/Off/Reboot	X		X		X
Serial Over LAN (Console Redirection)			X		X
OEM Customization	X	X	X		

4.5.1   Intel® Multi-Server Manager

The Intel® Multi-Server Manager is a product offering from the Intel® System Management Software - a suite of software products designed to reduce the cost and time of managing servers and keep businesses running 24/7.

Intel® Multi-Server Manager is included with almost all Intel Server Products at no additional charge giving user "peace of mind" that servers are healthy.

Prime benefits include:

Proactive alerting. Allows the server administrator to plan routine maintenance activities and avoid unplanned downtime.

Asset inventory. Tells you what components are installed in the server without having to shut down and open the system.

Remote debug. Isolates problems quickly saving hours and even days in the time it takes to debug and fix the issue.

Additional features bring in benefits including:

Simple discovery and grouping capabilities. Discovery of the system regardless of the operating system and organize them exactly how you want to.

Power on, off, or reset the servers from a remote location.

Single point alert configuration. Set up email alerting for all the systems in your environment from one location.

Powerful reporting. Select from many reports to run against a single system or an entire group. Compare two or more servers to see systems differences.

Many ways to use Intel® Multi-Server Manager:

- Manage Intel® Active System Console (version 4.4 or above) directly
- Manage Intel® MSM Agent
- Manage Intel® Agentless (out-of-band)
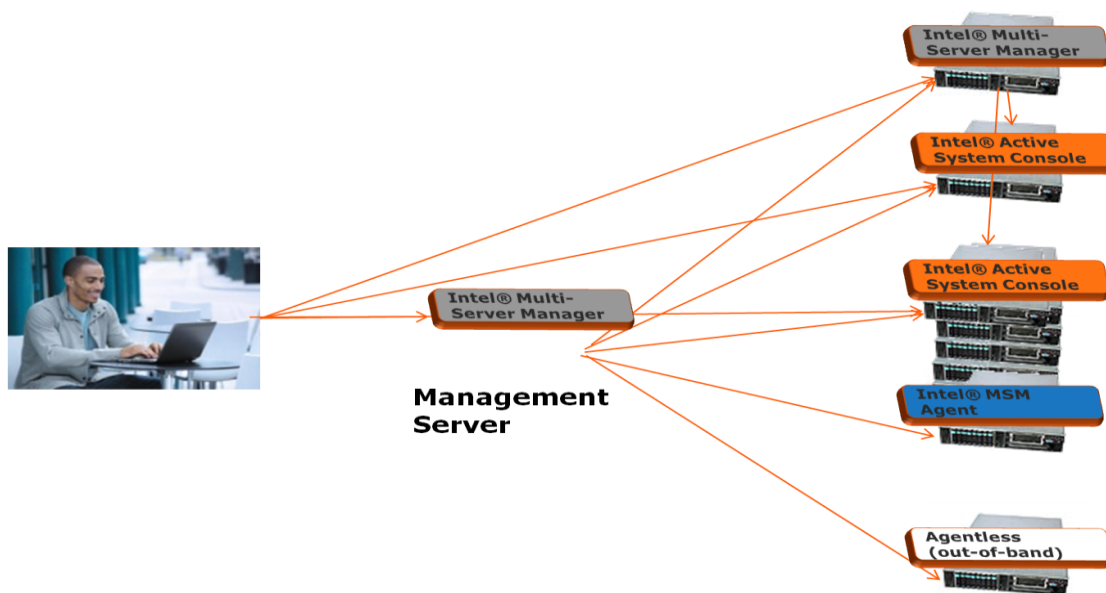
Figure 20. Intel® Multi-Server Manager

4.5.2   Intel® Active System Console

The Intel® Active System Console is a simple, lightweight web application console that gives you a dashboard view of the Server hardware on which it is running. It helps you proactively monitor the health of your Server, allows remote configuration of Server, tracking of assets, alerting of any issues and generation of asset reports.

The Intel® Active System Console is a product offering from the Intel® System Management Software - a suite of software products designed to reduce the cost and time of managing servers and keep businesses running 24/7.

IASC is included with almost all Intel® Server Products at no additional charge giving your customer "peace of mind" that servers are healthy.

IASC offers the following:

- Proactive alerting allows the server administrator to plan routine maintenance activities and avoid unplanned downtime

- Asset Inventory tells you what components are installed in the server without having to shut down and open the system

- Remote debug isolates problems quickly saving hours and even days in the time it takes to debug and fix the issue.

Figure 21. Intel® ASC Home Page

The Intel® Active System Console displays the hardware sensors, Field Replaceable Unit (FRU) data, and System Event Log (SEL) for the Intel Computer selected in the Intel Computers view. This console is only available for Intel servers that have an ESB2 BMC or Integrated BMC.

To launch the Intel® Active System Console, go to Start > Programs > Intel® Server Management Software > Intel® Active System Console.

Apart from system healthy monitoring, IASC also provides you with system configuration capability, such as the LAN channels of the BMC, set BMC User's password, change boot configuration, change power restore configuration, and Serial Over LAN configuration. Configuration of node manager policies is also allowed in IASC.

For detailed information, refer to the *Intel® Active System Console User Guide* that is included in the

Intel® SMS DVD.

4.5.3   Intel Management Packs

Intel® SMS features an integrated installer that packages the three Intel management packs in a single solution. The management packs are:

- Intel® Server Management pack version
- Intel® Modular Server Management pack version
- Intel® AMT Management pack for AMT Clients

4.5.3.1   Intel® Server Management Pack

The Intel® Server Management Pack for Microsoft System Center Essentials 2007* SP1 provides hardware monitoring capabilities to Intel Servers that support IPMI version 2.0. This Management Pack works on both Microsoft System Center Essentials* and Microsoft System Center Operations Manager*.

The Intel® Server Management Pack consists of the following components:

- Intel® Server Management Pack
- Intel® Server Management Agent

The Intel® Server Management Pack has the following features:

- Adds Intel® Agent Managed and Agentless Computers to the Microsoft System Center Essentials 2007* Monitoring views
- Provides a new hardware event log in the Windows* operating system Event Viewer
- Launches Intel® Command Line Interface (Intel® CLI), and a Serial Over LAN (SOL) console from the Microsoft System Center Essentials 2007* console
- Supports Intelligent Platform Management Interface (IPMI) based Intel servers
- Supports remote power control and system reset
- Provides power usage graphs for Power Supply Management Interface (PSMI)-supported agent-based servers
- Supports graceful power off and reset when the operating system and management agent are present
- Supports remote BMC configuration from within the Intel® Server Management Pack console and Intel® CLI.
- Includes the Intel® Server Management Pack Console that shows you sensor readings, Field Replaceable Unit (FRU) data, and the System Event Log (SEL) for the selected Intel computer
- Supports "Maintenance Mode" in Microsoft System Center Essentials 2007* and Microsoft System Center Essentials 2010*.
- Provides monitoring of server hardware parameters like CPU, memory, hard disks, and RAID status
- Health Monitoring of servers discovered both in in-band and out-of-band states

For detailed information on usage of the Intel® Server Management Pack, refer to the *Intel® Server Management Pack User Guide*.

4.5.3.2 Intel® Modular Server Management Pack

The Intel® Modular Server Management Pack provides essential server management tools for small and medium-sized businesses. This Management Pack adds server management functionality for Intel® Modular Server platforms by building upon the extensive capabilities of Microsoft System Center Essentials 2007*.

The Intel® Modular Server Management Pack has the following features:

- Discovery Configuration Wizard detects networked Intel® Modular Server systems.
- Displays the health and alerts from Intel® Modular Server Compute Modules.
- Supports launching the Intel® Modular Server Control Software web-based console.

For detailed information on usage of Intel® Module Server Management Pack, refer to the *Intel® Modular Server Management Pack User Guide*.

4.5.3.3 Intel® AMT Management Pack

Intel® AMT Management pack is used to manage AMT enabled Intel® Desktop systems.

For detailed information on usage of Intel® AMT Management pack, you have to refer to Intel AMT Management pack User Guide.

4.5.4 Intel Command Line Interface

The Intel® Command Line Interface console, called dpccli, runs on the management console and enables communication between the management console and the network proxy, which in turn communicates to the managed server.

The Intel® Command Line Interface uses a network proxy (dpcproxy) that runs on the managing client system or on a central network proxy. The network proxy is installed by the Intel® System Management Software installation program provided with your Intel server.

4.5.4.1 DPCCLI Features and Benefits

The Intel® Command Line Interface lets you control a server from the command line rather than from a graphical user interface. You can enter Intel® Command Line Interface commands at a command prompt or from a script file to do the following:

- Remotely power on or off a server
- Remotely reset the server
- Request machine identifiers
- Read sensor values
- Display the network configuration of the BMC
- IPMI 1.0, 1.5 and 2.0 authentication support
- Packet encryption based on IPMI version

You can use any of the following consoles to launch dpccli or telnet and issue Intel® Command Line

Interface commands:

- The Window's command-line environment (command prompt)
- A Linux* command shell

4.5.4.2 Using DPCCLI

The Intel® Command Line Interface tool has two modes: Platform Control mode and Serial Over LAN (SOL) Console Redirection mode.

Platform control mode

When the Intel® Command Line Interface is in Platform Control mode, you can issue commands to the remote system.

To start an Intel® Command Line Interface session with dpccli, the network proxy dpcproxy must be running, either on the managing console or a central network proxy system. However, by default you should not have to do anything for the network proxy to be running, because the installation program installs the network proxy and sets it up for automatic start upon reboot.

Serial Over LAN (SOL) mode

When the Intel® Command Line Interface is in SOL Console Redirection mode, you can perform, over a LAN connection, any activity you could at the remote system's console, including viewing the remote system's console output (SOL allows data from the server serial port to be redirected over the LAN).

The Serial over LAN Console Redirection mode of Intel® Command Line Interface lets servers transparently redirect the serial character stream from the baseboard UART to and from the managing client system over the LAN. Serial over LAN has the following benefits compared to a serial interface:

- Eliminates the need for a serial concentrator
- Reduces the amount of cabling
- Allows remote management of servers without video, mouse, or keyboard (headless servers)

For a command prompt console, you must start dpccli before you can access the Intel® Command Line Interface commands. The dpccli executable file acts as an interface between the console and the network proxy. Once the interface is started, you can then connect to a server and enter commands.

4.5.4.3 DPCCLI versus Telnet

There are two basic ways to issue Intel® Command Line Interface commands through the network proxy to a remote server: by using the console interface, called dpccli; or by using telnet. Both methods are described in detail in the *DPCCLI User Guide*.

DPCCLI

An Intel® Command Line Interface session over dpccli requires a server name (or address) and login (user and password), which can be supplied as arguments to the dpccli command.

Telnet

When using telnet to connect to the remote server (to issue Intel® Command Line Interface commands and to operate in SOL mode), you must connect the telnet session to the dpcproxy by specifying (in the telnet

command line) the port on which dpcproxy is listening.

Once the Intel® Command Line Interface session over dpccli is running and the connection to the intended server is established, you can begin issuing Intel® Command Line Interface commands to that server at the dpccli prompt. If connecting through telnet, the same dpccli prompt is displayed when in Platform Control mode (default), and you can issue Intel® Command Line Interface commands at the dpccli prompt over telnet.

4.5.4.4 Using telnet for both Platform Control and SOL Modes

Serial over LAN mode requires a telnet session from the managing console to the Network Proxy server, regardless of which operating system (Microsoft Windows* or Linux*) you are running on either system. Start the telnet session to the remote server as follows:

- At the operating system command prompt, type
  ```
  telnet xxx.xxx.xxx.xxx 623 <Enter>
  ```

  The xxx represent the IP address of the system running the Network Proxy. This may be a central network server with the Proxy installed. If you are connecting to the local system, use "localhost" instead of the system's IP Address. The 623 represents the default Port address required for Intel® Command Line Interface connections. If this port address has been changed while executing the dpcproxy command, use that port address. For example: telnet 10.7.162.58 623 or telnet localhost 623

- At the "Server:" prompt, provide the IP Address or DNS Name of the server to which you want to connect.

- Provide the BMC username and password for the target system.

After authentication is performed, you will see a login successful message and the dpccli> prompt (even over telnet, Intel® Command Line Interface starts in Platform Control mode by default). You can now enter Intel® Command Line Interface commands or switch to SOL Console Redirection mode.

For the latest Intel® Command Line Interface information, including system requirements and supported operating systems refer to the *Release Notes* and *Intel® Command Line Interface User Guide* provided with your Intel® System Management Software or Intel® Server Management Software CD or DVD.

4.5.5 Intel SNMP subagent

Intel® SNMP Subagents are SNMP extension agents that provide interfaces and databases for retrieving server hardware information and for monitoring server health status on the network using the SNMP protocol.

The Management Information Base (MIB) file that accompanies each SNMP subagent contains the definitions of the management information the SNMP subagent can access, with each definition distinguished by a unique object identifier (OID). Each SNMP subagent has its own MIB file and OID. The SNMP subagents support SNMP-based access (GETs, SETs and TRAPs) to the instrumented components on the managed server, collecting and returning information as requested by a management system.

The subagents plug into the SNMP Master Agent infrastructure supported by the operating system and

respond to queries and sets filtered to the subagents by the master agent, based on the OID specifying the data defined in the MIB to be retrieved or set.

4.5.5.1 SNMP Master Agent

You must install the SNMP Master Agent on the managed server.

- For supported Linux* operating systems, use the net-snmp package.
- For supported Microsoft Windows* operating systems, use the SNMP Service included in the Microsoft Windows* operating system.

For systems running the Microsoft Windows* operating system, the SNMP subagent is implemented as a dynamic link library (DLL) and is configured in the Registration Database.

For Linux* systems, the SNMP subagent is implemented as an rpm package. It is installed, configured and started as a service. The SNMP master agent (net-snmp) communicates with the subagent through Agent protocol.

4.5.5.2 Install the Intel SNMP Subagent

For Microsoft Windows* operating system-based systems, the SNMP service (available on the operating system installation CD) must be installed first. The autorun software on the Intel® System Management Software CD provides links for the installation of tools and utilities. These links lead you to SNMP subagent installation.

To install the Intel® SNMP Subagents on a Linux* system, run the install script installed with the Intel® SNMP Subagent:

./snmpsubagentinstall.sh

✎ **NOTE**

The Installation Instructions on the Intel® System Management Software CD contains installation instructions for all the Intel® utilities.

4.5.5.3 Features of the Intel® SNMP Subagent

Through basic SNMP GETs, SETs, and TRAPs, the Intel® SNMP Subagent provides the following functionality for managing servers:

- Accessing sensor data
- Viewing and modifying threshold settings
- Reading the SMBIOS tables
- Providing overall system health status

For detailed information on how to configure SNMP subagent and use SNMP subagent for server health monitoring, refer to the *Intel® SNMP Subagent User Guide* that is provided with Intel® System Management Software CD or DVD.

4.6 Other Tools

In addition, the BMC can be accessed by standard, off-the-shelf terminal or terminal emulator utilities such as open source IPMITOOL, IPMIUtility, and FreeIPMI that allow access to sensor status information, and power control.

The end user owns the risk of using un-validated open source utilities.

5 Scenarios and Best Practices

This chapter provides examples that show how to make the Intel® Server Management Interface to work. Topics covered in this chapter include:

- Configure BMC for OOB function using SYSCFG
- Configure BMC for OOB function using IDA
- Remotely manage Intel server use DPCCLI

5.1 Configure BMC using SYSCFG

To enable the BMC for out-of-band communication over a LAN connection, at a minimum you will need to configure the following settings:

- IP source (static or DHCP)
- IP Address
- Subnet mask
- Default gateway (only required if you will be connecting from client outside of subnet)
- Enable one user
- Enable user's privilege level
- Set users and passwords
- Enable text-based console redirection (serial Over LAN - SOL) if needed

5.1.1 Configure BMC users

Step-by-step instructions to use SYSCFG to configure BMC user authorization:

- Set password for BMC user 1 (Anonymous) by typing:
  `syscfg /u 1 "" "password"` (password is "password" in this example)
- Enable the BMC user 1 on BMC channel 1 by typing:
  `syscfg /ue 1 enable 1`
- Enable "admin" privilege and payload type to "SOL" for the BMC user 1 on BMC channel 1 by typing:
  `syscfg /up 1 1 admin  sol`

5.1.2 Configure BMC for LAN connection

To use SYSCFG to configure BMC LAN connection, perform the following step:

- Configure the LAN channel IP info on BMC channel 1 by typing:
  syscfg /le 1 static 192.168.1.12x 255.255.255.0

5.1.3   Configure BMC to use SOL

To enable the BMC for SOL connection, at a minimum you will need to configure the following settings:

- Set up one user

- Enable a LAN channel for SOL

- Enable a user for SOL

To use SYSCFG to configure BMC SOL, perform the following step:

- Enable Serial Over LAN (SOL) on BMC channel 1 by typing:
  syscfg /sole 1 enable admin 115200 5 60
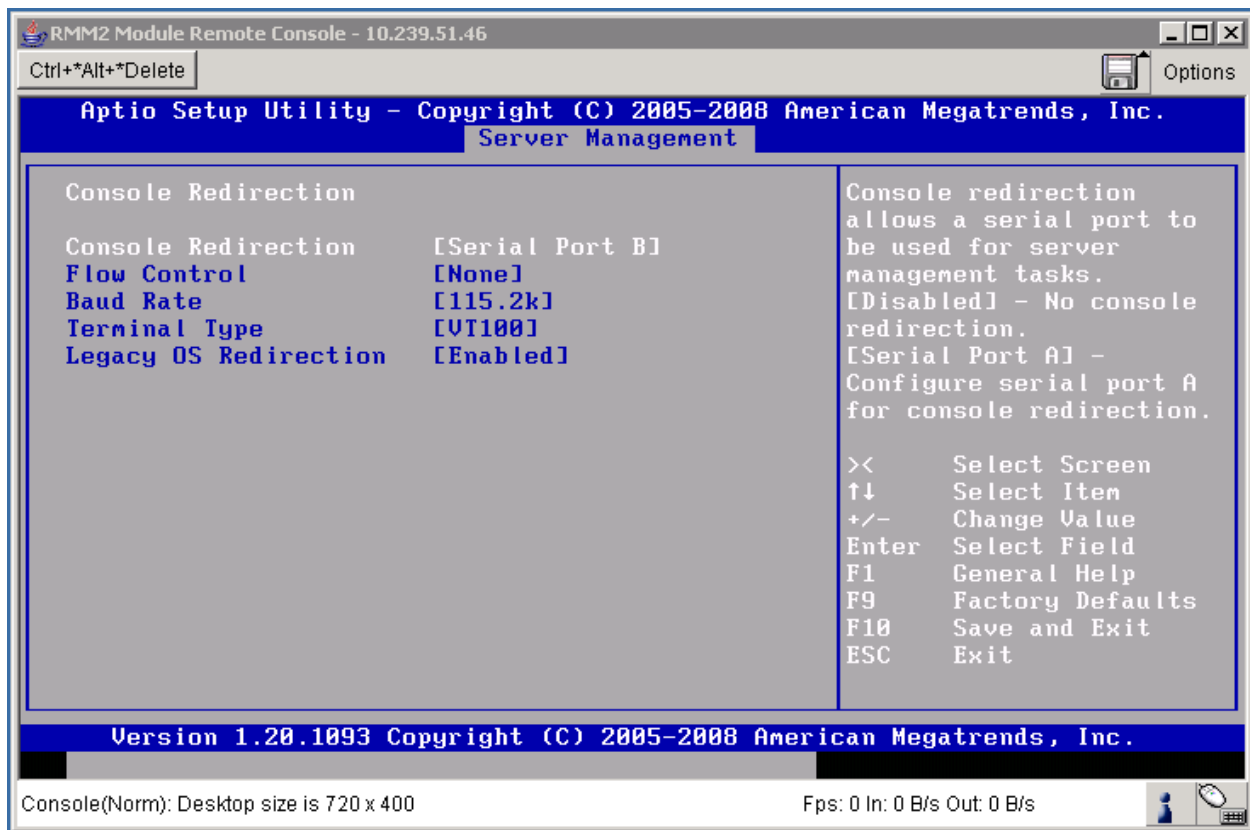
Figure 22. Configure Console Redirection for Serial B

5.2   Configure the BMC using IDA

Intel® Deployment Assistant Software is provided on the Intel® Server Deployment Toolkit CD that is shipped with the system. With IDA, it is easy to configure the BMC using the Graphical User Interface (GUI).

5.2.1   Configure BMC for LAN connection

To use the IDA to configure OOB LAN, perform the following steps:

- Select "Configure a Server" after booting from the IDA CD.

- Select "Server Management Settings" and click the "Next" button.

- Click "LAN Channel 1 (onboard NIC1)" if you want to configure BMC LAN channel 1, and click the "Next" button.

✏ **NOTE**

You can also select "LAN Channel 2" depending on your configuration.

- Select "IP Address from a DHCP Server" or "Static IP Address" for BMC LAN Channel IP and key in your IP address/Subnet Mask/Gateway depending on your network configuration.
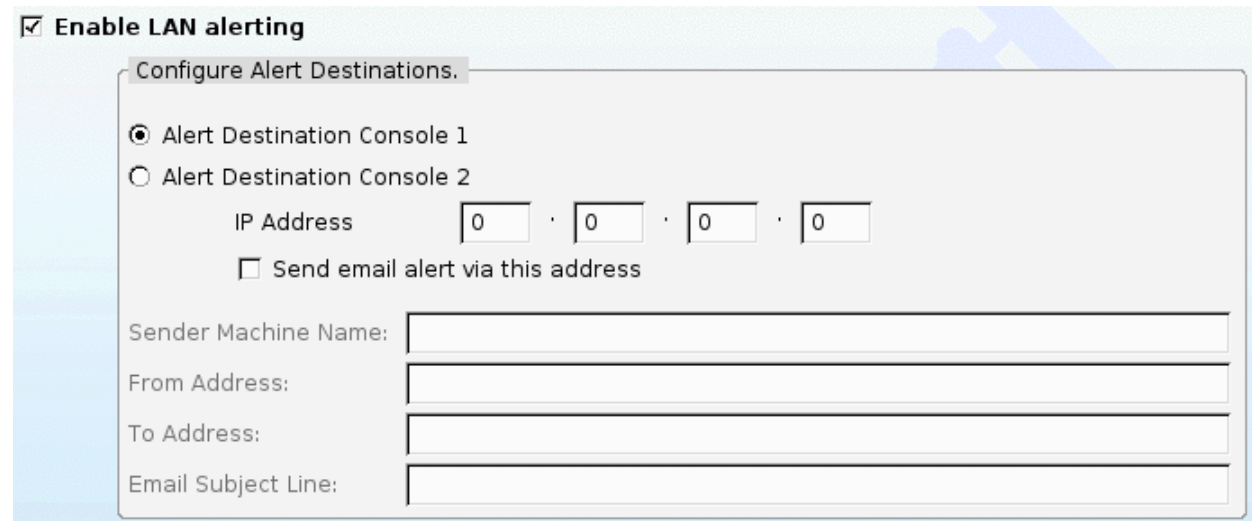
5.2.2   Configure BMC to use SOL

To use IDA to configure SOL, select "Enable Serial Over LAN".

5.2.3   Configure BMC for embedded email alerts

To use IDA to configure email alerts, perform the following steps:

- Select "Enable LAN alerting".

- Configure Alert Destinations by selecting "Alert Destination Console 1" or "Alert Destination Console 2".

- Enter the IP Address and select the "Send email alert through this address" check box if you want to send an email alert through this address.

- Enter the "Sender Machine Name", "From Address", "To Address" and "Email Subject Line" depending on your email alert configuration.

Figure 23. Enable LAN Alerting

5.2.4   Configure BMC Platform Event Filters

To use IDA to configure PEF filters, perform the following steps:

- Select the check boxes for the events that are to trigger alerts as shown in the following figure.

Figure 24. Configure BMC PEF

- Click the "Next" button to move on to the next configuration page.

5.2.5   Configure BMC users

To use IDA to configure users perform the following steps:

- Select the "Anonymous User" line and click the "Edit" button to configure BMC anonymous user.

⮫   **NOTE**

You can configure other BMC users depending on your preference.
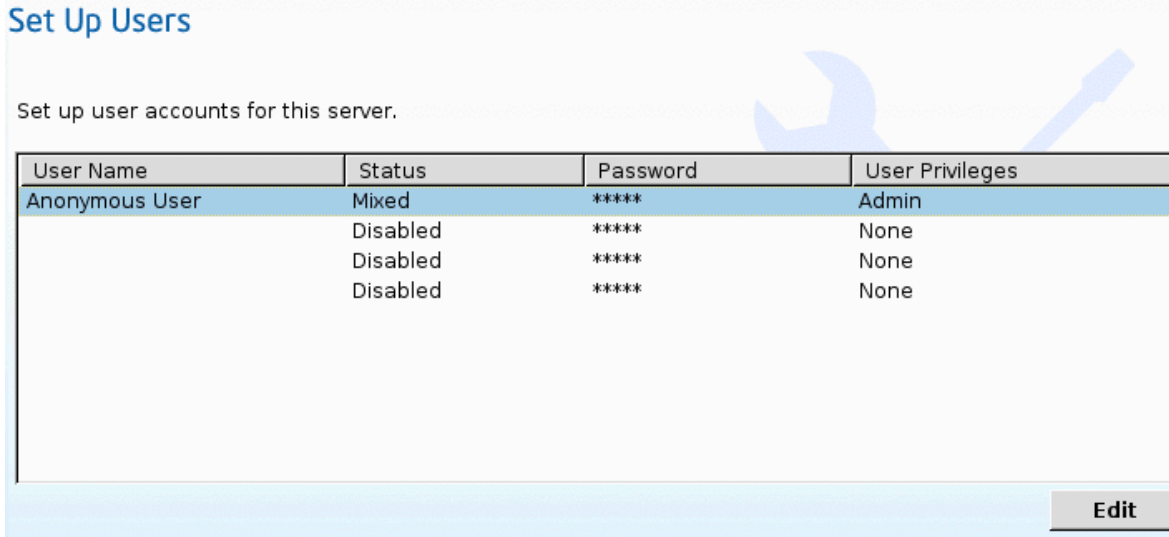
Figure 25. Configure BMC Users

- In the "Edit User Data" dialog box, you can enable the user account you selected and assign user privileges to this user. Make sure to select the "Change Username and Password" check box and enter the password and confirm the password. Then, click the "OK" button.
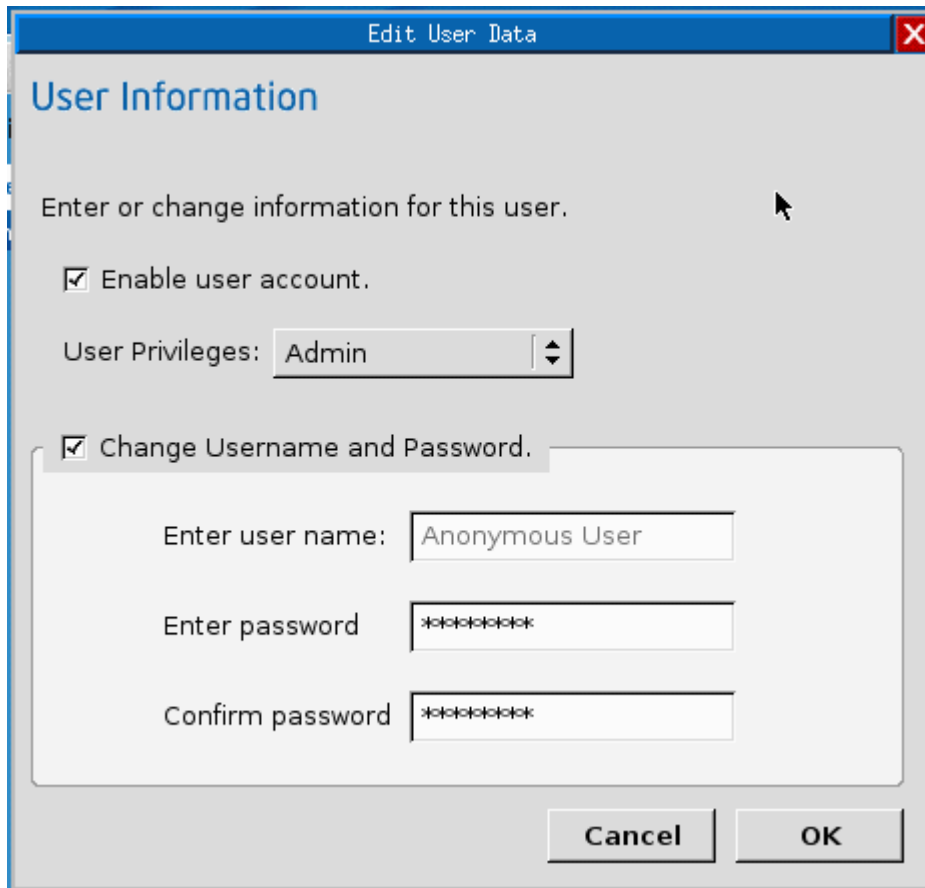
Figure 26. Set BMC user's password

- Apply the configuration and click "Restart" to reboot the server.

This will save the configuration that is applied.

5.3   Configure basic Integrated BMC setting from BIOS menu

Starting from Intel® Server Board S5500 and S3420 platforms, we have enabled BMC basic setting (IP address, username and password) to be done from BIOS menu. The sub-menu is called "BMC LAN configuration":

Figure 27. BMC LAN Configuration

5.3.1   Configure BMC for LAN connection

When prompted on boot, press F2 to display the BIOS menu:

- Move "Server Management" section of BIOS menu
- And then go to BMC LAN configuration sub-menu

```
Aptio Setup Utility - Copyright (C) 2009 American Megatrends, Inc.
                      Server Management

 Baseboard LAN configuration                        Select BMC IP source. When
 IP source                    [Dynamic]             static option is selected, IP
 IP address                   10.239.56.134         address, subnet mask and
 Subnet mask                  255.255.255.0          gateway are editable. When
 Gateway IP                   10.239.56.241         dynamic option selected, these
                                                    fields are read-only and IP
 Intel (R) RMM3 LAN configuration                   address is acquired
 Intel (R) RMM3               Present               automatically (DHCP).
 IP source                    [Static]
 IP address                   192.168.1.13
 Subnet mask                  255.255.255.0
 Gateway IP                   0.0.0.0

 BMC DHCP host name
                                                    →←     Select Screen
 User configuration                                 ↑↓     Select Item
 User ID                      [anonymous]           +/-    Change Value
 Privilege                    [Administrator]       Enter  Select Field
 User status                  [Enable]              F1     General Help
 User name                    anonymous             F9     Optimized Defaults
 User password                                      F10    Save and Exit
                                                    ESC    Exit

          Version 1.23.1114. Copyright (C) 2009 American Megatrends, Inc.
```

Figure 28. BMC IP Configuration

- Go to "Baseboard LAN configuration" or "Intel® RMM3 LAN configuration" area.
- Choose "Dynamic" or "Static" to either configure DHCP or static IP Address for BMC LAN channel 1 or Intel® RMM3 LAN channel 3
- Modify Subnet mask and Gateway IP as needed

5.3.2   Configure BMC users

To use BIOS menu to configure users perform the following steps:

Go to "BMC LAN configuration" sub-menu under "Server Management" section of BIOS menu

Move to "User configuration" section and chose "anonymous" user or "root" user:

✏   **NOTE**

You can configure other BMC users depending on your preference.

```
         Aptio Setup Utility - Copyright (C) 2009 American Megatrends, Inc.
                        Server Management

                                                        Select the user id to configure.

   Baseboard LAN configuration
   IP source                      [Dynamic]
   IP address                     10.239.56.134
   Subnet mask                    255.255.255.0
   Gateway IP                     10.239.56.241

   Intel (R) RMM3 LAN configuration
   Intel (R) RMM3                 Present
   IP source                      [ ┌──── User ID ────┐
   IP address                     1 │ anonymous        │
   Subnet mask                    2 │ root             │
   Gateway IP                     0 │ User3            │
                                    │ User4            │
   BMC DHCP host name               │ User5            │
                                    └──────────────────┘
   User configuration                                   →←       Select Screen
   User ID                        [anonymous]           ↑↓       Select Item
   Privilege                      [Administrator]       +/-      Change Value
   User status                    [Enable]              Enter    Select Field
   User name                      anonymous             F1       General Help
   User password                                        F9       Optimized Defaults
                                                        F10      Save and Exit
                                                        ESC      Exit


         Version 1.23.1114. Copyright (C) 2009 American Megatrends, Inc.
```

Figure 29. Configure BMC Users

✏ **NOTE**

The User ID "anonymous" cannot be used through the RMM3 interface.

- Select the "Enable" to enable "root" user account (here is an example)
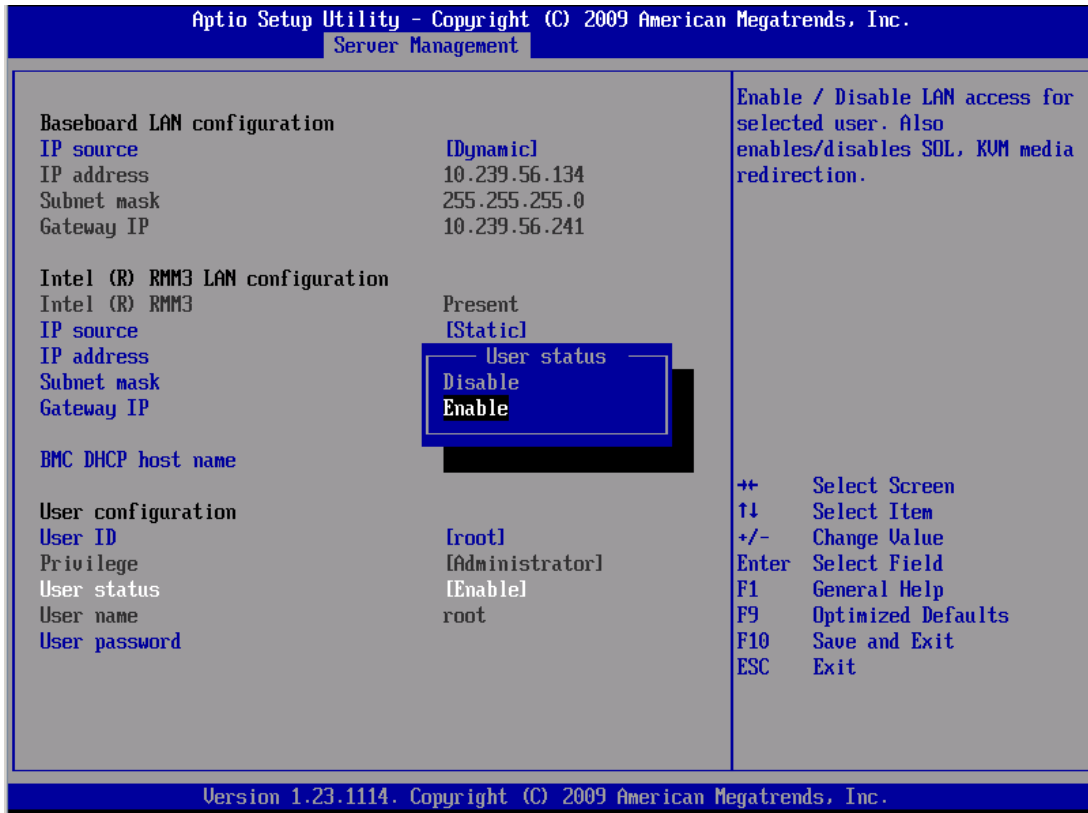
Figure 30. Enable BMC user

- Create and confirm user's password:
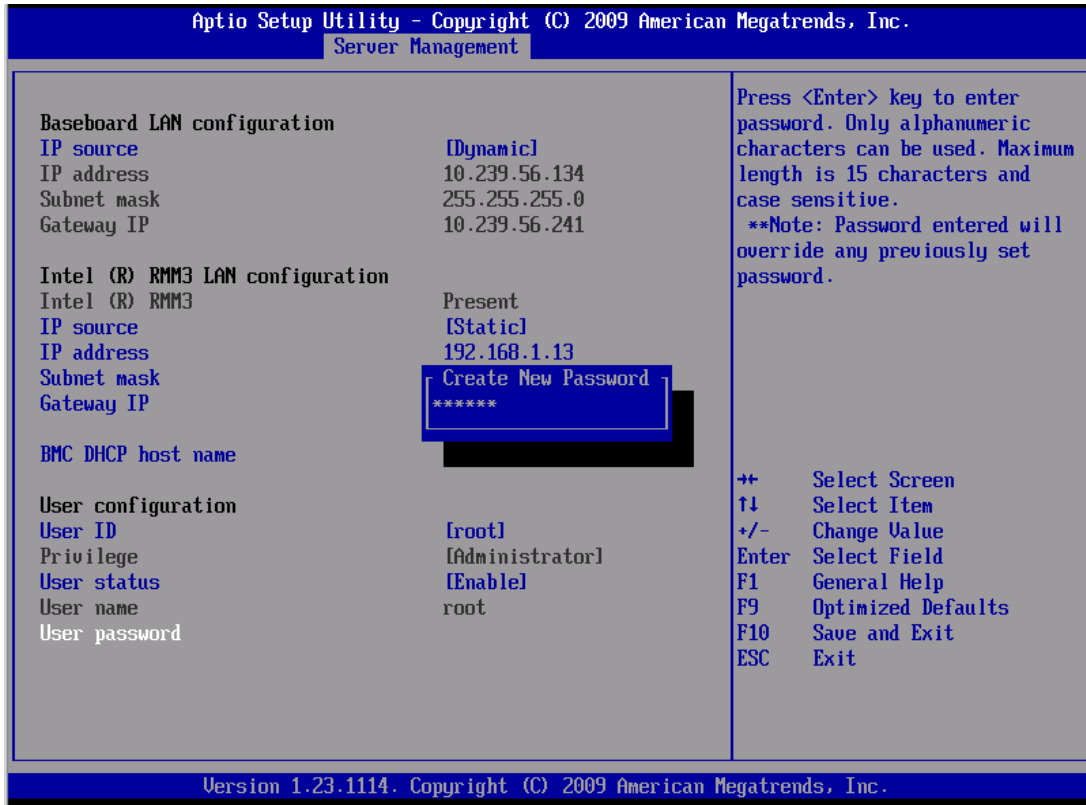
Figure 31. Set BMC user's password

- Confirm the changes by press F10, "Save configuration and Exit"

```
        Aptio Setup Utility - Copyright (C) 2009 American Megatrends, Inc.
    ◄ Error Manager  Exit

        Save Changes and Exit                          Exit BIOS Setup Utility after
        Discard Changes and Exit                       saving changes. The system will
                                                        reboot if required.
        Save Changes                                   The [F10] key can also be used.
        Discard Changes

        Load Default Values
        Save as User Default Values
        Load User Default Values
                          ─ Save & Exit Setup ─
                          Save configuration and exit?

                              Yes        No          →     Select Screen
                                                     ↓     Select Item
                                                     +/-   Change Value
                                                     Enter Select Field
                                                     F1    General Help
                                                     F9    Optimized Defaults
                                                     F10   Save and Exit
                                                     ESC   Exit


        Version 1.23.1114. Copyright (C) 2009 American Megatrends, Inc.
```

Figure 32. Save BMC settings

✎ **NOTE**

BMC LAN Channel setting change only take effect after next reboot by pressing F10 to "Save configuration and Exit".

5.4 Remotely Manage the Server through DPCCLI

The Intel® Command Line Interface (CLI) console runs on the management console and enables communication between the management console and the network proxy, which in turn communicates to the managed server. The Intel® Command Line Interface lets you control a server from the command line rather than from a graphical user interface. You can enter Intel® Command Line Interface commands at a command prompt or from a script file to do the following:

- Remotely power on or off a server or reset the server
- Read sensor values
- Operate remote server in SOL mode

5.4.1 Configuring BIOS and BMC

Before you can use DPCCLI to manage a remote server through SOL for access the BIOS boot up screen,

at a minimum you will need to configure the following settings on the BMC and BIOS of the remote server:

- IP source (static or DHCP), IP Address, Subnet mask

- Enable one user and set password for this user

- Enable user's privilege level

- Enable text-based console redirection (serial Over LAN - SOL)

ESB2 BMC and Integrated BMC may have a different default BMC setting; you must check/configure the following settings if you encounter an issue when pinging the BMC and connecting to the BMC through DPCCLI:

✏ **NOTE**

SYSCFG for Linux* is used to display these settings as examples; you can either use SYSCFG for EFI/Windows or IDA.

- Ensure the BMC ARP Response is enabled.

If this setting is not enabled, you may not be able to ping ESB2 BMC's IP address. To enable it, type `#syscfg /lc 1 enable 10b`

Integrated BMC has this setting enabled by default.

```
linux-ml6q:/usr/local/syscfg # ./syscfg /d lan 1
LAN Configuration Settings:
--------------------------
LAN Channel Selected: 1
LAN Alert Destination Index Selected: None. LAN Alert Configuration
will not be displayed.

IP Address Source: Static
BMC Host IP Address: 192.168.1.19
Subnet Mask: 255.255.255.0
Gateway IP Address: 0.0.0.0
Gateway MAC Address: 00-00-00-00-00-00
Backup Gateway IP Address: 0.0.0.0
Backup Gateway MAC Address: 00-00-00-00-00-00
Community String:
Gratuitous ARP Enable: Enabled
Gratuitous ARP Interval (milliseconds): 2000
BMC ARP Response Enable: Enabled
linux-ml6q:/usr/local/syscfg #
```

Figure 33. Gratuitous ARP and BMC ARP Response Setting

- Ensure that the configured Channel "Access Mode" is set as "Always".

- If this setting is set, you may not be able to see the BIOS boot information from SOL for ESB2 BMC. To enable it, type #syscfg /lc 1 7 Always

- Integrated BMC has this setting enabled by default.

```
linux-ml6q:/usr/local/syscfg # ./syscfg /d channel 1
Channel Configuration Settings
------------------------------
Channel Selected: 1
Channel Type: LAN
Features Supported: Basic Lan & SMTP

Authentication Types:
---------------------
Callback: [Not Configured]
User: [Not Configured]
Operator: [Not Configured]
Administrator: [Not Configured]

Per Message Authentication: Enabled
User Level Authentication: Enabled
Access Mode: Always
Privilege Level: Admin
PEF status: Disabled
linux-ml6q:/usr/local/syscfg # █
```

Figure 34. BMC LAN Channel Access mode

5.4.2   Install DPCCLI to the management console

For the latest information on the Intel® Command Line Interface, including system requirements and supported operating systems, refer to the *Release Notes* provided with your Intel® System Management Software or Intel® Server Management Software CD.

To install DPCCLI, go to the "Utilities" directory, double-click IntelStandaloneUtils-x86_64.exe, select English, and then select Custom Install and install CLI only:
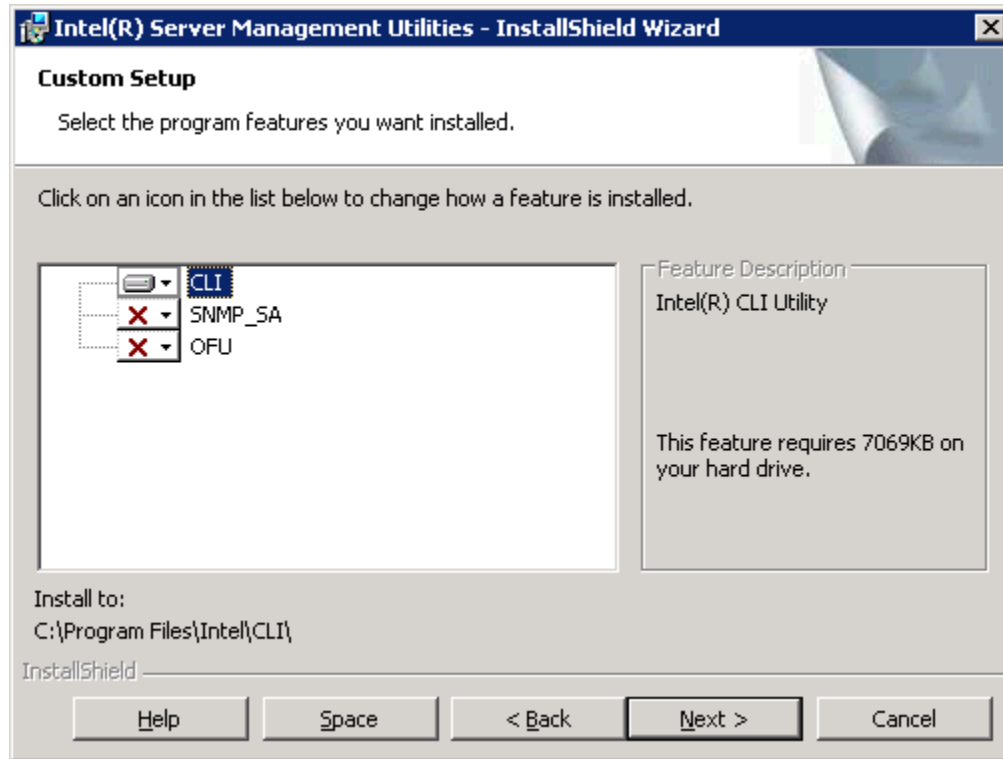
Figure 35. Intel® DPCCLI Installation

If you are installing DPCCLI on Microsoft Windows 2008* system, you must enable telnet service in your management console.

5.4.3   Remote manage server by DPCCLI

You must first complete the steps detailed in section 5.2 or 5.4 to enable the BMC for OOB and SOL connection. Then, you can connect the managed server using DPCCI.

You can use Telnet to remotely manage the server. When using telnet to connect to the remote server (that is, to issue Intel® DPCCLI commands and to operate in SOL mode), you must connect the telnet session to the dpcproxy by specifying (in the telnet command line) the port on which dpcproxy is listening as follows:

- On the management system, double-click the Telnet Localhost 623 desktop icon.
  You will now able to connect to the managed server
- At the server prompt, type the assigned Integrated BMC IP Address that you previously configured (for example: Server: xxx.xxx.xxx.xxx).
- At the username prompt, press the <Enter> key.
  You are logging in under the anonymous user account. No user name is assigned.
- At the password prompt, enter "password".
  This password was assigned when you configured BMC OOB function.

* "Login successful" should be displayed on your screen.
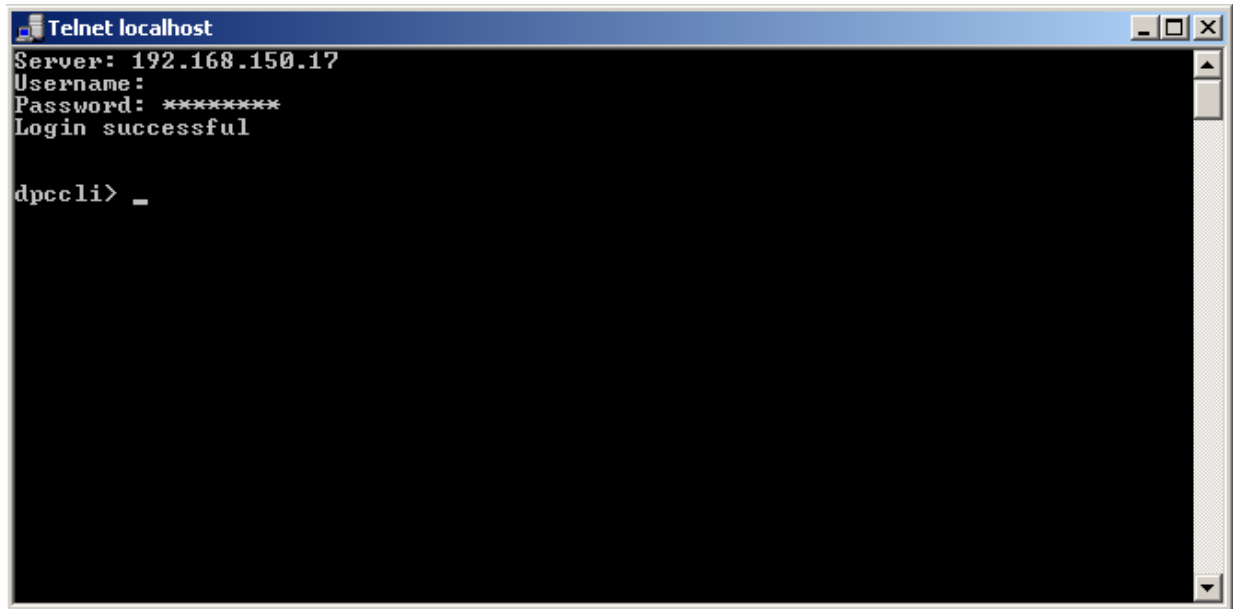
Figure 36. DPCCLI login screen

The following tasks demonstrate some of the features of the Intel® Command Line Interface utility. This includes monitoring system information, retrieving and saving the system event log and starting a SOL session.

1. To read the temperature sensors of the remote managed system, type:

   dpccli> `sensors -v -T temp`

11/14/2008	13:58:32	Baseboard Temp	ok	28.00	Celsius
11/14/2008	13:58:32	P1 Mem Margin	ok	1.00	Celsius
11/14/2008	13:58:32	IOH Therm Margin	ok	-28.00	Celsius
11/14/2008	13:58:33	P2 Mem Margin	ok	0.00	Celsius
11/14/2008	13:58:33	P1 Therm Margin	ok	-64.00	Celsius
11/14/2008	13:58:33	P2 Therm Margin	ok	-61.00	Celsius

2. To read the fan speeds of the remote managed system, type:

   dpccli> `sensors -v -T fan`

11/14/2008	13:59:09	Processor 1 Fan	ok	6120.00	RPM
11/14/2008	13:59:09	Processor 2 Fan	ok	6120.00	RPM
11/14/2008	13:59:09	Memory 1 Fan	ok	0.00	RPM
11/14/2008	13:59:09	Memory 2 Fan	ok	4152.00	RPM
11/14/2008	13:59:09	System 1 Fan	ok	0.00	RPM
11/14/2008	13:59:09	System 2 Fan	ok	2688.00	RPM
11/14/2008	13:59:09	System 3 Fan	ok	0.00	RPM
11/14/2008	13:59:09	System 4 Fan	ok	2832.00	RPM

   dpccli>

3. To read all system sensors, type:

    dpccli> `sensors -v`

11/14/2008 | 13:58:03 | BB +1.1V IOH	| ok	| 1.28	| Volts
11/14/2008 | 13:58:04 | BB +1.1V P1 Vccp	| ok	| 0.84	| Volts
11/14/2008 | 13:58:04 | BB +1.1V P2 Vccp	| ok	| 0.84	| Volts
11/14/2008 | 13:58:04 | BB +1.5V P1 DDR3	| ok	| 1.52	| Volts

    dpccli>

You can use the Intel® Command Line Interface to display and save the system event log on remote management clients.

1. To display and save the System Event Log (SEL) in text format on the remote system (where the dpcproxy is running), type:

    dpccli> `displaylog -F csv -O c:\UR.sel`

    …

    1,Pre-Init Time-stamp ,Processor #0x60,Processor Presence detected

    2,Pre-Init Time-stamp ,Processor #0x61,Processor Presence detected

    3,Pre-Init Time-stamp ,Power Unit #0x01,Power Off/Down

    4,Pre-Init Time-stamp ,Power Unit #0x01,Power Off/Down

    5,Pre-Init Time-stamp ,System Event #0x83,Timestamp Clock Synch. Event Is First Of Pair.SEL TimeStamp Updated.

    6,11/14/2008,11:20:42,System Event #0x83,Timestamp Clock Synch. Event Is Second Of Pair. SEL TimeStamp Updated.

    7,11/14/2008,11:21:47,System Event #0x01,OEM System Boot Event

    dpccli>

This saves the System Event Log (SEL) to c:\UR.sel on the remote management console.

2. To view the SEL, open the UR.sel file in notepad. (Open Windows Explorer on the management console (laptop) and right-click the UR.sel file and open with notepad.)

3. To save the SEL to HEX format remotely, type:

    `displaylog -F hex -O c:\UR.sel`

5.4.4   Using SOL to access BIOS Menu

When the ESB2 BMC or Integrated BMC are used for serial port sharing, SOL and Console Redirection on the Serial B port are mutually exclusive features, but SOL setting and console redirection setting must be synced.

In order to access the BIOS Setup Menu from a SOL session, you may have to configure BIOS console redirection as a pre-request.

You can use Telnet to remotely manage the server. When using telnet to connect to the remote server (that is, to issue Intel® DPCCLI commands and to operate in SOL mode), you must connect the telnet

session to the dpcproxy by specifying (in the telnet command line) the port on which dpcproxy is listening as follows:

- To remote power-off the managed system, type:

  dpccli> power –off

- To power on the managed system and start a SOL session, type:

  ```
  dpccli> power -on –console
  ```

- Monitor the managed system's BIOS boot up screen through Serial Over LAN (SOL).

  Example: Press "F2" go to BIOS menu and select "Discard Changes and Exit".
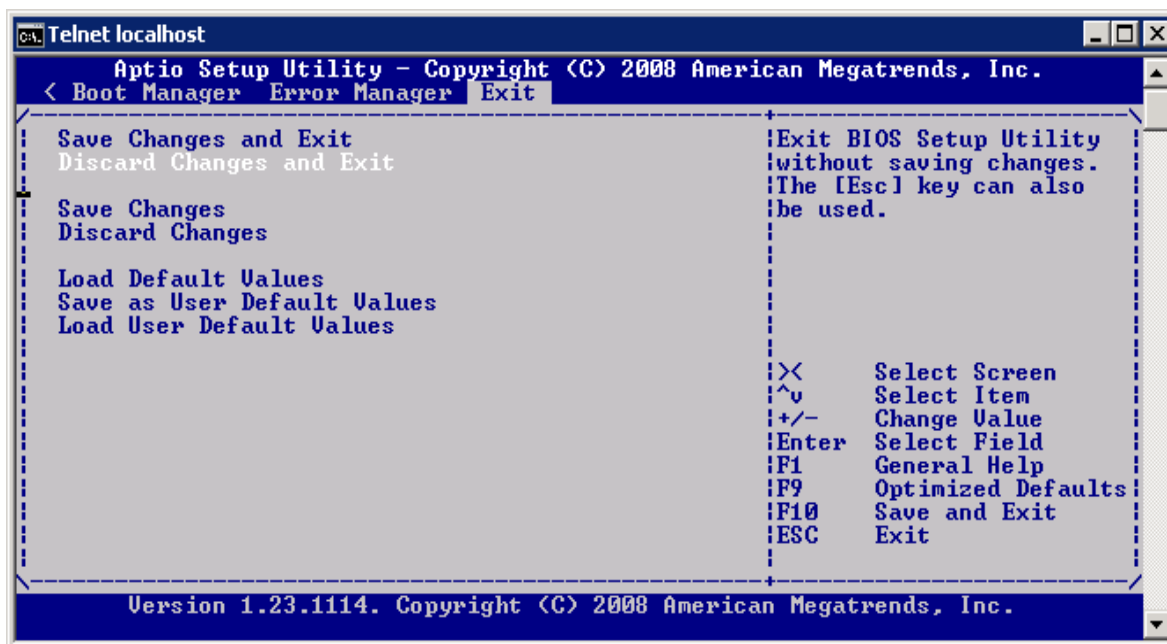
Figure 37. BIOS menu screen under SOL

- Close the "Telnet localhost" window.

5.4.5   Configuring Microsoft Windows Server 2003* to support

SOL

When you connect to the BMC using the DPCCLI, you can remotely control the text console. With SOL, this also includes operating systems such as Microsoft Windows Server 2003* and Linux*.

Windows Server 2003 has two components that work with DPCCLI and the BMC to provide out-of-band access to the operating system:

- Microsoft Emergency Messaging Service* (EMS)

- Microsoft Special Administration Console* (SAC)

To exit SOL and return to the SMBridge prompt, press the tilde key and the period key (that is, press ~.).

For more information, see:

http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS_SAC_commands.asp

To enable EMS on a Microsoft Windows Server 2003*, do the following.

- Log in to Windows as an administrator.

- Launch a command prompt and enter the command **bootcfg**.

Figure 38. Bootcfg display with default Windows default setting

- Examine the output. If there is more than one boot entry, then you need to determine the default entry by looking at the default line under Boot Loader Settings and determine whether Boot Entry has a matching Path value. In the example shown in Figure 38 there is only one boot entry, 1.

- Issue the following command, substituting your boot entry number in the /id parameter if it is not 1 as in the example shown:

```
bootcfg /ems on /port com2 /baud 115200 /id 1
```


Figure 39. Enable Windows EMS on Serial Port 2

✏ **NOTE**

> In order to perform this step, you must enable console redirection on COM2 (SOL session) with a
> baud rate of 115200 in advance for this setting (115200 baud rate is only used as an example in
> this guide).
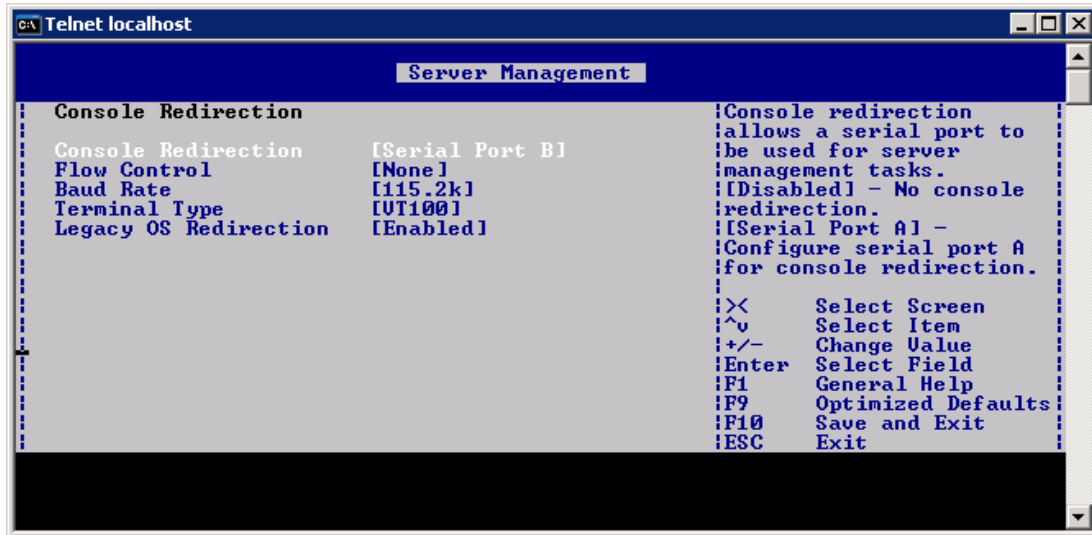
Figure 40. Console Redirection on Serial Port B

- Reissue the bootcfg command to see the result. The changes are highlighted in the example shown.
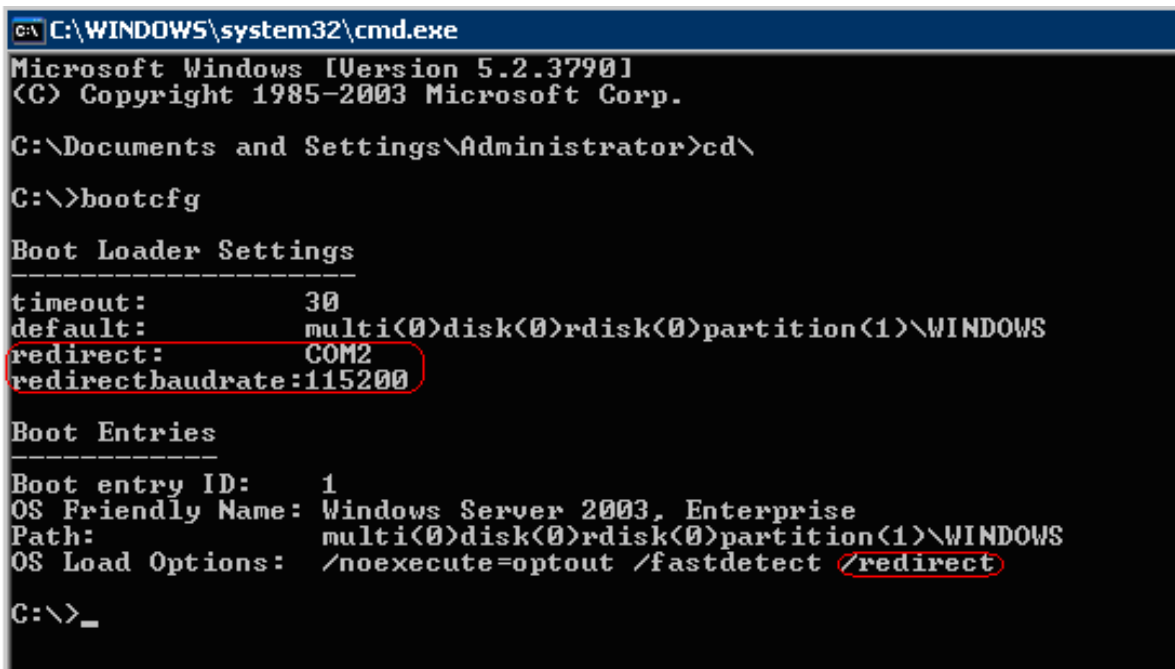
Figure 41. EMS setting results

- Reboot the server in order for the changes to take affect.

NOTE

To turn EMS off again, issue the following command:

```
bootcfg /ems off /id 1
```

Where 1 is the boot entry you modified in the preceding steps. Reboot the server to bring the changes online.

• Once you reboot and engage the DPCCLI console, you will see the EMS console.

• **Tip:** After you start the DPCCLI console, if you only get a blank screen, press the <Enter> key a few times to get the SAC> prompt.

You can now issue the various SAC commands.
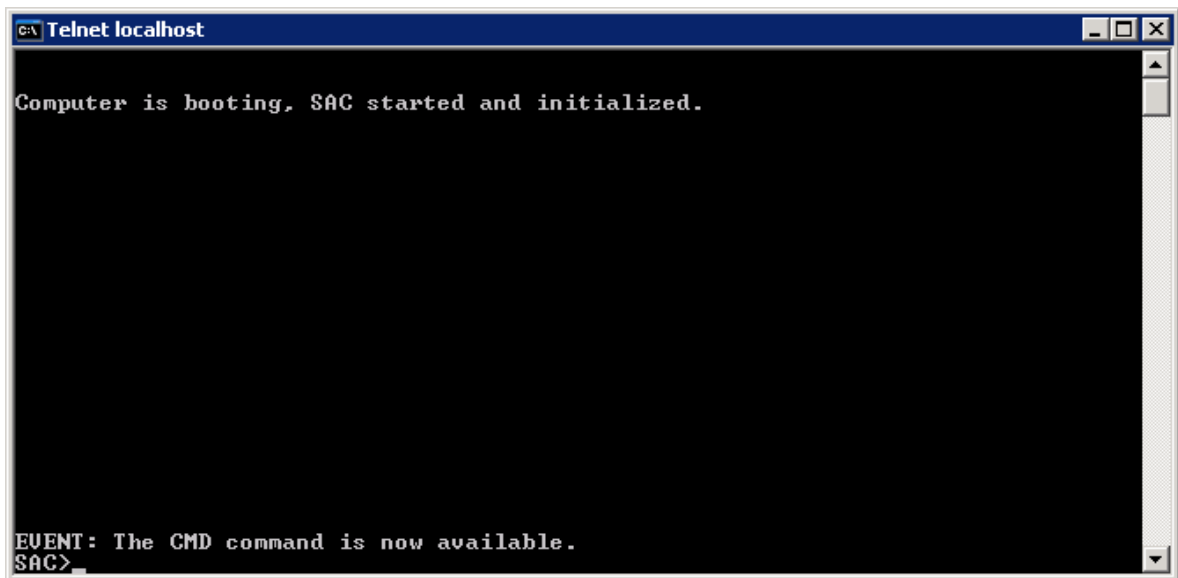
Figure 42. EMS Console

• Type the "ch –si" command to log in to the Windows OS command line environment.

NOTE

In the Login screen, key in username/domain name/password for authorization.

Now, you are under the Windows Command Line Prompt:

```
EVENT: The CMD command is now available.
SAC>cmd
The Command Prompt session was successfully launched.
SAC>
EVENT:    A new channel has been created.  Use "ch -?" for channel help.
Channel: Cmd0001
SAC>ch
Channel List

(Use "ch -?" for information on using channels)

# Status   Channel Name
0 (AV)     SAC
1 (AV)     Cmd0001
SAC>_
SAC>ch -si 1_
```

```
Please enter login credentials.
Username: Administrator
Domain  : bsce1
Password: ******_
```

```
Telnet localhost

(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>_
```

Figure 43. Login into Windows command line prompt

- To close the command prompt channel, type exit.
- To leave the channel open and return to the SAC prompt, press <Esc>+<Tab>+0 (the number zero) (three keys in sequence).
- To leave the remote console and return to DPCCLI, press <tilde>+<period> (that is, ~.)

5.4.6 Configuring Linux* to support SOL

You must configure Linux* to expose the Linux* initialization (booting) process through SOL. This enables users to log in to the Linux* console through an SOL session and direct output to the serial console.

In this guide, SuSE* Linux is provided as an example. The solution for Red Hat* Linux is quiet similar.

Apart from the minimum setting described in Section 5.4.1 to allow SOL to access the BIOS boot up menu, the SOL Baud Rate setting needs to be consistent with the GRUB setting under Linux*.

```
linux-ml6q:/usr/local/syscfg #
linux-ml6q:/usr/local/syscfg # ./syscfg /d sol 1
SOL Configuration Settings:
--------------------------
Channel Number Selected: 1
SOL Enable: Enabled
Privilege Level Limit: Admin
Baud Rate (bits/second): 115200
Retry Count: 5
Retry Interval (ms): 60
linux-ml6q:/usr/local/syscfg #
```

Figure 44. Baud Rate setting for SOL

To configure SuSE* Linux to support SOL, follow these steps:

- Log in as root.
- Change GRUB GUI setting to text mode to display the GRUB menu in the SOL console by modifying the /boot/grub/menu.lst file as follows:

  Comment out the gfxmenu line and add the "display" line as shown.

```
# Modified by YaST2. Last modification on Sat Feb 14 02:19:16
default 0
timeout 8
# gfxmenu (hd0,5)/boot/message
display (hd0,5)/boot/message
```

Figure 45. Change GRUB GUI to be displayed through SOL

- Enable Linux* boot procedure to be seen in the SOL console by adding the following lines for SOL boot session (an example is as shown below):

title SUSE Linux Enterprise Server 10 SP2 SOL Session

root (hd,5)

kernel /boot/vmlinuz-2.6.16.60-0.21-bigsmp root=/dev/bi-id/scsi-SATA_ST31600811AS_6PT03YN8-part vga=0x314 acpi=off resume=/dev/sda5 splash=slient showtpts console=ttyS1,19200 console=tty1

initrd /boot/initrd-2.6.16.60-0.21-bigsmp

The result is shown in the following image:

```
###Add SOL boot option###
title SUSE Linux Enterprise Server 10 SP2 SOL Session
     root (hd0,5)
     kernel /boot/vmlinuz-2.6.16.60-0.21-bigsmp root=/dev/disk/by-id/
scsi-SATA_ST3160811AS_6PT03YN8-part6 vga=0x314    acpi=off resume=/d
ev/sda5 splash=silent showopts console=ttyS1,115200n console=tty1
     initrd /boot/initrd-2.6.16.60-0.21-bigsmp

###Don't change this comment - YaST2 identifier: Original name: linu
x###
title SUSE Linux Enterprise Server 10 SP2
     root (hd0,5)
     kernel /boot/vmlinuz-2.6.16.60-0.21-bigsmp root=/dev/disk/by-id/
scsi-SATA_ST3160811AS_6PT03YN8-part6 vga=0x314    acpi=off resume=/d
ev/sda5 splash=silent showopts
     initrd /boot/initrd-2.6.16.60-0.21-bigsmp
```

Figure 46. GRUB file with SOL session added

✎ **NOTE**

For Red Hat* Linux, SOL console device may be **ttyS0**. It depends on your Linux* version and configuration. "rhgb quiet" needs to be removed to allow you view the boot up information from the SOL console.

4. Enable users to log in from SOL console by modifying the /etc/inittab file to add the following line:

```
S0:12345:respawn:/sbin/agetty -L 115200 ttyS1 vt102
```

This allows gettys through ttyS1 in standard runlevels section and enable users to log in at the SOL console.

The result is shown in the following image:

```
#
#S0:12345:respawn:/sbin/agetty -L 9600 ttyS0 vt102
S0:12345:respawn:/sbin/agetty -L 115200 ttyS1 vt102
#cons:12345:respawn:/sbin/smart_agetty -L 38400 console

#
```

Figure 47. Enable users login at SOL console

5. Allow users to log in as root from the SOL console by modifying the /etc/securetty file to add the following line:

```
ttyS1
```

The result is shown in the following image:

```
# without leading /dev/) on which root is allowed to login.
#
tty1
ttyS1
tty2
tty3
tty4
tty5
tty6
```

Figure 48. Enable users login as root from SOL console

6. Reboot Linux* to see the GRUB menu from SOL console.
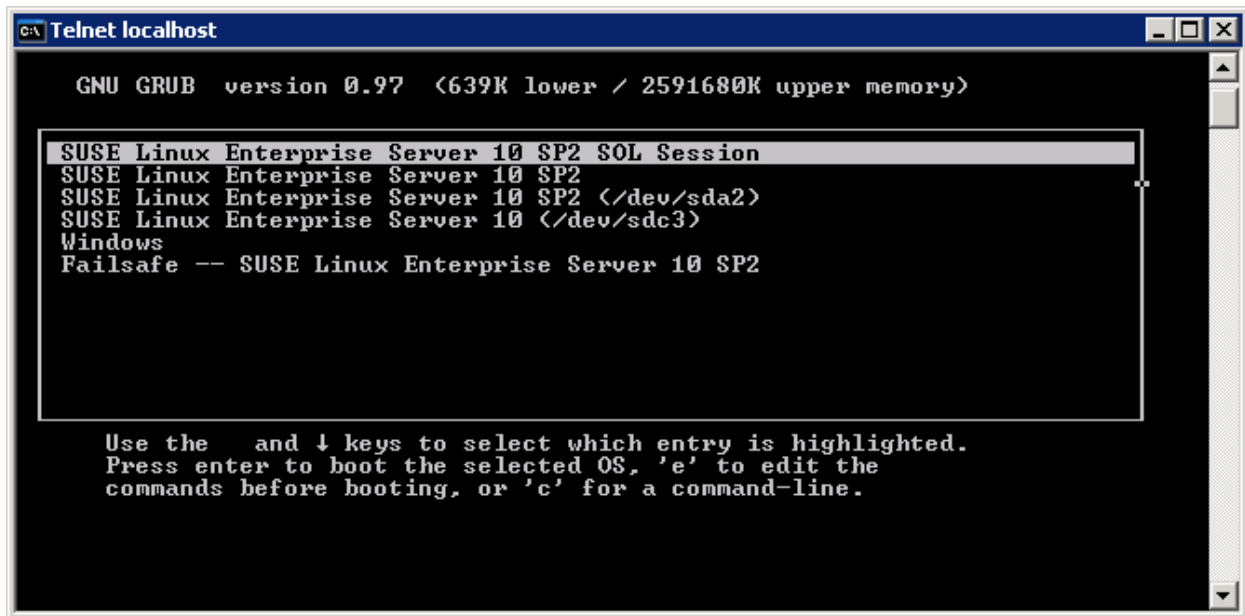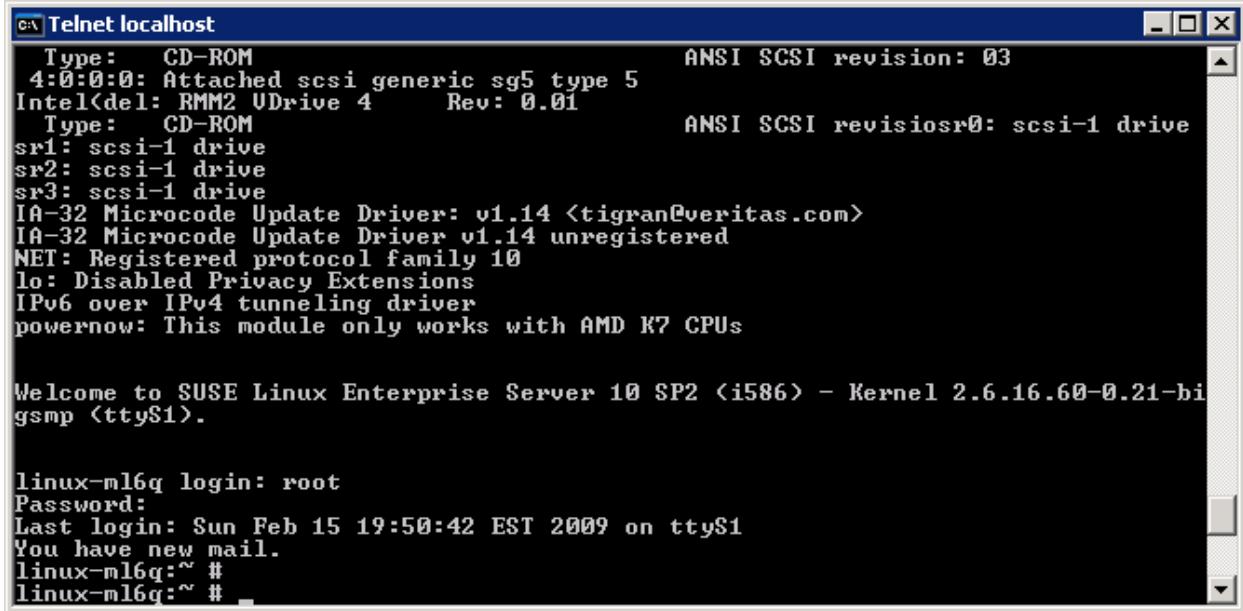
Figure 49. TXT GRUB interface from SOL console

The following figure displays the Linux* SOL login console:

Figure 50. SuSE Linux* SOL login console

5.5 Managing Server using SMASH

The **Systems Management Architecture for Server Hardware** (SMASH) is a suite of specifications that deliver industry-standard protocols to increase productivity of the management of a data center. The SMASH Command Line Protocol (SM CLP) specification provides an interface to heterogeneous servers, independent of machine state or OS state, system topology or access method. It is a standard method for local and remote management of server hardware using out-of-band communication.

SMASH is being developed by the Distributed Management Task Force (DMTF) Server Management Working Group (SMWG). For more details about SMASH, see: http://www.dmtf.org/standards/smash

Intel® S5000 Series Server Boards and Intel® S5500 Series Server Boards and Intel® S1200BT Series Server Boards support an interface to System Management Architecture for Server Hardware (SMASH) and the associated Command Line Protocol (CLP) when advanced features are enabled (that is. with Intel® RMM2, Intel® RMM3 or Intel® RMM4 module installed).

5.5.1 Logging into the SMASH* Session

1.   ssh to BMC from the client machine.

2.   SMASH console screen ('•') should appear. If not execute '/usr/local/bin/smash' from the # prompt.

3.   This executable will initialize all the needed variables, discover the targets and will show the SMASH console screen.

5.5.2   SMASH* Targets

SMASH* Targets is the first layer of the SMASH* which contains two targets. They are settings1 and system1. The settings1 contains all the current session supported values and the system1 is the server/blade and about this target is explained in the next section.

5.5.3   Supported Properties

The supported property of the SMASH* target is identity.

Property	Task
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

The supported property of the SMASH* target is identity.

Property	Task
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.3.1   Supported Verbs

Following are the supported verbs of the SMASH* targets:

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
show	Show all the targets, properties, and verbs supported by this target.
version	Show the current version of SMASH*.

```
                      >> SMASH-CLP Console v1.09 <<
->show
COMMAND COMPLETED :
show

 ufip=/
  Targets:

        settings1/
        system1/

  Properties:
       identity=root


  Verbs:
       cd
       exit
       help
       show
       version


->
```

Figure 51. SMASH* Target

5.5.4   System1

The system target represents the server/blade. Power control is available on the target .System1, It contains sol1, sp1, and other sensor monitoring targets. Here sp1 means Service Process Configuration.

5.5.4.1   Supported Properties

The supported properties of the target system1 are as follows:

Property	Task
CurrentPowerStatus	This Read-Only property shows the power status of the system as ON or OFF.
	The value of the property is assigned to any of the following values:
	ON - If the power status of the system is on, then the value of this property is ON.
	OFF - If the power status of the system is off, then the value of this property is OFF.
SysIdSupported	This read only property indicates if System Identification is
	SUPPORTED or NOT SUPPORTED
SysIdentification	This R/W property reflects the current state of system identification.
	It can set to any of the following values:
	System identification can be turned off as follows: ->Set SysIdentification=OFF
	System identification can be timed ON as follows: ->Set SysIdentification=TIMED
	Set the timeout value. The TimeOutValue property is set to TIMED and SysIdentification property value is set to ON.
	Note: If set SysIdentification=INDEFINITE, then TimeOutValue property is set to INDEFENITE and SysIdentification property value is set to ON.
TimeOutValue	This value is R/W, which is associated with TIMED (ON) gives input in seconds as follows:
	INDEFINITE - System identification is ON for an indefinite period of time.
	TIMED –System identification is ON for only a known period of time.
	OFF- System identification is currently OFF.
	If TimeOutValue is TIMED then set the TimeOutValue to ->Set TimeOutValue=3 (only numeric, non zero values accepted).
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.4.2   Supported Verbs

The supported verbs of the system1 targets are as follows:

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
set	Set the R/W supported properties.
reset	Reset the R/W supported properties

show	Show all the targets, properties, and verbs supported by this target.
start	Start the device.
stop	Stop the device.
version	Show the current version of SMASH*.

```
->show
COMMAND COMPLETED :
show

 ufip=/system1
  Targets:

        sensor2/
        sol1/
        sp1/
        system2/
        system3/
        system4/
        pwrsupply1/

  Properties:
        CurrentPowerStatus=ON
        SysIdSupported=SUPPORTED
        SysIdentification=OFF
        TimeOutValue=INVALID
        identity=host


  Verbs:
        cd
        exit
        help
        reset
        set
        show
        start
        stop
        version

->
```

Figure 52. System Target

```
->set sysidentification=TIMED
COMMAND COMPLETED :
set sysidentification=TIMED

 ufip=/system1
       sysidentification=TIMED
Please set the Timeoutvalue for timed on

->set TimeOutValue=3
COMMAND COMPLETED :
set TimeOutValue=3

 ufip=/system1
       TimeOutValue=3

->show
COMMAND COMPLETED :
show

 ufip=/system1
  Targets:

       sensor2/
       sol1/
       sp1/
       system2/
       system3/
       system4/
       pwrsupply1/

  Properties:
       CurrentPowerStatus=ON
       SysIdSupported=SUPPORTED
       SysIdentification=ON
       TimeOutValue=TIMED
       identity=host


  Verbs:
       cd
       exit
       help
       reset
       set
```

Figure 53. Example of System Target

5.5.5   Settings1

Settings1 target represents the settings of the current session of SMASH* and does not have any targets.

This target affects the current session:

5.5.5.1   Supported Properties

The supported properties of the target Settings1 as follows:

Property	Task
cdt	Represents the current default directory. This is the path from where the session starts.
outputformat	This R/W property gives the output format: clpxml, text, clpcsv. Keyword of the current running SMASH* session. The values supported by this property are explained as follows: • **Clpxml** - The output format of the current running SMASH* session is in the .xml format ->set outputformat=clpxml • **Keyword**- The output format of the current running SMASH8 session is in the keyword format ->set outputformat=keyword. • **Text**- The output format of the currently running SMASH session is in the text format->set outputformat=text. By default, this property value is assigned to text. • **Clpcsv** – This output format of the currently running SMASH* session has a "clpcsv" table to represent the Command Status. Each line of the "clpcsv" output data has its first item either as the "header" or as the "group" keyword. Rows beginning with the "header" keyword specify the start of a new table and the items in the comma-separated list of keywords identify the output data elements that appear in each row of the table. Rows beginning with the "group" keyword specify a row of table values for the preceding header.
timeout	• The R/W property timeout represents the inactivity timeout value in seconds of the currently running SMASH* session. If the SMASH* session is inactive for the timeout value seconds mentioned, then after reaching the timeout value this session will exit automatically. The value of this property can be set to a preferred inactivity time. ->set timeout=300. By default, it is assigned to 500.
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.5.2   Supported Verbs

The supported verbs of the settings1 target are as follows:

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
set	Set the R/W supported properties.
show	Show all the targets, properties, and verbs supported by this target.
version	Show the current version of SMASH*.

Figure 54. Setting1 Target

5.5.6 SP1

The SP1 target (service processor) provides information of the user accounts Ethernet port and logs. It contains three targets -- enetport1 (Ethernet port target), accounts, and logs.

5.5.6.1 Supported Properties

The supported property of the SMASH* target is identity.

Property	Task
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.6.2 Supported Verbs

The supported verbs of the SP1 target are as follows:

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
show	Show all the targets, properties, and verbs supported by this target.
version	Show the current version of SMASH*.

```
->show
COMMAND COMPLETED :
show

 ufip=/system1/sp1
  Targets:

        account10/
        account1/
        account2/
        account3/
        account4/
        account5/
        account6/
        account7/
        account8/
        account9/
        enetport1/
        logs1/

  Properties:
        identity=service processor


  Verbs:
        cd
        exit
        help
        show
        version

->
```

Figure 55. SP1 Target

5.5.7   SOL1

Serial Over LAN (SOL) is the name for the redirection of baseboard serial controller traffic over an IPMI session. It does not have any targets.

5.5.7.1   Supported Properties

The supported property of the target SOL1 is as follows:

Property	Task
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.7.2 Supported Verbs

The supported verbs of the SOL1 target are as follows:

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
show	Show all the targets, properties, and verbs supported by this target.
start	Start the device.
version	Show the current version of SMASH*.

```
->cd sol1
COMMAND COMPLETED :
cd sol1

 ufip=/system1/sol1

->show
COMMAND COMPLETED :
show

 ufip=/system1/sol1
  Properties:
        identity=serial redirection


  Verbs:
        cd
        exit
        help
        show
        start
        version


->
```

Figure 56. SOL1 Target

5.5.7.3 Terminating an SOL Session

SOL session can be terminated using the following control key sequence:

CR, ESC, T or t

CARRIAGE RETURN/ENTER key, followed by ESCAPE key, followed by T or t

Control key sequence 'Ctrl+ [can be used in place of ESCAPE key].

Once terminated, the control returns to SMASH-Lite* session.

5.5.8   Enetport1

The BMC in the managed system needs the system's IP Address and MAC Address in order to be able to respond to UDP/IP packets or generate LAN alerts. Enetport1 (Ethernet port target) gives the port address information. Enetport1 contains only one target named lanendpt1.

5.5.8.1   Supported Properties

The supported properties of the target enetport1 are as follows:

Property	Task
macaddress	Address that was received by the activated session. This read only property gives the value of the MAC address. Mac address is a unique identifier attached to most network adaptors (NICs).
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.8.2   Supported Verbs

The supported verbs of the Enetport1 target are as follows:

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
show	Show all the targets, properties, and verbs supported by this target.
version	Show the current version of SMASH*.

```
->show
COMMAND COMPLETED :
show

 ufip=/system1/sp1/enetport1
  Targets:

        lanendpt1/

  Properties:
      macaddress=00:5A:4A:3C:2E:41
      identity=ethernet port


  Verbs:
      cd
      exit
      help
      show
      version

->
```

Figure 57. Enetport1 Target

5.5.9   Lanendpt1

The target Lanendpt1 gives information about LAN configuration. It contains the target:

Ipendpt1 - IP configuration.

5.5.9.1   Supported Properties

Following is the supported property of target lanendpt1:

Property	Task
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.9.2   Supported Verbs

The supported verbs of the Lanendpt1 target are as follows:

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
show	Show all the targets, properties, and verbs supported by this target.
start	Start the device.
version	Show the current version of SMASH*.

```
->show
COMMAND COMPLETED :
show

 ufip=/system1/sp1/enetport1/lanendpt1
  Targets:

        ipendpt1/

  Properties:
        identity=lan information


  Verbs:
        cd
        exit
        help
        show
        version

->
```

Figure 58. LANENDPT1 Target

5.5.10   Ipendpt1

The target Ipendpt1 provides information about ipaddress and other information related to the SP. It contains two targets - dnsendpt1 and remotesap1. The supported properties and supported verbs of the Ipendpt1 are as follows.

5.5.10.1   Supported Properties

The supported properties of the target ipendpt1 are as follows:

Property	Task
Ipaddress	The value of ipaddress is the IP address of the SP. An IP address (Internet Protocol address) is a unique address that is used to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). This is an R/W property. The value setting to the ipaddress affects the IP of the SP. ->set ipaddress=10.0.4.79 This will change the ipaddress of the sp. After changing, use committed property to save.
Subnetmask	This is the value of the subnetmask of the SP. A subnetmask is a range of logical addresses within the address space that is assigned to an organization. This is an R/W property. The value setting to the ipaddress affects the IP of the SP. ->set subnetmask=255.255.248.0 This will change the subnetmask of the sp. After changing, use committed property to save.
Usedhcp	Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices to obtain various parameters necessary for the networked devices to operate in an Internet Protocol(IP) network. This property has two values(1 for DHCP and 0 for Static). This is a R/W property. ->set usedhcp=1
Committed	Once the ipadress or subnetmask is set to 1, the property saves all the changes made. In addition, the network settings also change and network connection is lost. ->Set commited=1
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.10.2   Supported Verbs

The supported verbs of the Ipendpt1 target are as follows:

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
set	Set the r/w supported properties
show	Show all the targets, properties, and verbs supported by this target.
version	Show the current version of SMASH*.

```
->show
COMMAND COMPLETED :
show

 ufip=/system1/sp1/enetport1/lanendpt1/ipendpt1
  Targets:

        dnsendpt1/
        remotesap1/

  Properties:
        ipaddress=10.0.3.26
        subnetmask=255.255.248.0
        usedhcp=1
        committed=1
        identity=network parameters

  Verbs:
        cd
        exit
        help
        set
        show
        version

->
```

Figure 59. IPENDPT1 Target

5.5.11   Remotesap1

The remotesap1 target will enumerate all the configurable IPs under the containing target. A remote access server enables users who are not on a local network to access. This does not contains any targets.

5.5.11.1   Supported Properties

The supported properties of the target remotesap1 are as follows:

Property	Task
defaultgatewayaddress	IP address of the gateway. A gateway address is a private address and is the address to which traffic is sent from the LAN .This is an R/W property. The value of the gateway can be set as follows: ->Set defaultgatewayip=0.0.0.0
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.11.2   Supported Verbs

The supported verbs of the Remotesap1 target are as follows.

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
set	Set the r/w supported properties
show	Show all the targets, properties, and verbs supported by this target.
version	Show the current version of SMASH*.

```
->show
COMMAND COMPLETED :
show

 ufip=/system1/sp1/enetport1/lanendpt1/ipendpt1/remotesap1
  Properties:
       defaultgatewayaddress=0.0.0.0
       identity=remote server access point


  Verbs:
       cd
       exit
       help
       set
       show
       version

->
```

Figure 60. REMOTESAP1 Target

5.5.12 Dnsendpt1

The dnsendpt target has the configurable parameters for Domain Name System (DNS). The DNS associates various sorts of information with so-called domain names; most importantly, it serves the Internet by translating human-readable computer hostnames into the IP address, information that the networking equipment needs to deliver.Dnsendpt1 contains two targets - remotesap1 and remotesap2. The supported properties of dnsendpt1 are as follows.

5.5.12.1   Supported Properties

The supported properties of the target dnsendpt1 are as follows:

Property	Task
domainnamefromdhcp	Dhcp based DNS configuration. This property is a read only property.
dnsdomainname	This property gives the DNS Domain. This property is a read only property.
serversfromdhcp	This property shows the servers dhcp. This is a read only property.
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.12.2   Supported Verbs

The supported verbs of the Dnsendpt1 target are as follows.

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
show	Show all the targets, properties, and verbs supported by this target.
version	Show the current version of SMASH*.

```
->show
COMMAND COMPLETED :
show

 ufip=/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1
  Targets:

        remotesap1/
        remotesap2/

  Properties:
        domainnamefromdhcp=1
        dnsdomainname=Unknown
        serversfromdhcp=1
        identity=parameters of DNS


  Verbs:
        cd
        exit
        help
        show
        version

->
```

Figure 61. DNSENDPT1 Target

5.5.13 Remotesap1

The remotesap1 target enumerates all the configurable IPs under the containing target. A remote access server enables user access to those users who are not on a local network. This does not contain any targets.

5.5.13.1   Supported Properties

The supported properties of the target remotesap1 are dnsserveraddress and identity.

Property	Task
dnsserveraddress	This property gives the dns server address. This is a R/W property. The value of this property can be set as follows: ->set dnsserveraddress=0.0.0.0
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.13.2   Supported Verbs

The supported verbs of the remotesap1 target as follows:

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
set	Set the r/w supported properties
show	Show all the targets, properties, and verbs supported by this target.
version	Show the current version of SMASH*.

The remotesap1 target enumerates all the configurable IPs under the containing target. A remote access server enables users who are not on a local network to access. This does not contain any targets.

```
->show
COMMAND COMPLETED :
show

 ufip=/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap1
  Properties:
       dnsserveraddress=0.0.0.0
       identity=remote server access point


  Verbs:
       cd
       exit
       help
       set
       show
       version


->
```

Figure 62. REMOTESAP1 Target

5.5.14 Remotesap2

5.5.14.1   Supported Properties

The supported properties of the target remotesap2 are as follows:

Property	Task
dnsserveraddress	Gives the dns server address. This is a R/W property. The value of this property can be set as follows: ->set dnsserveraddress=0.0.0.0
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.14.2   Supported Verbs

The supported verbs of the remotesap2 target are as follows.

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
set	Set the r/w supported properties
show	Show all the targets, properties, and verbs supported by this target.
version	Show the current version of SMASH*.

```
->show
COMMAND COMPLETED :
show

 ufip=/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap2
  Properties:
      dnsserveraddress=0.0.0.0
      identity=remote server access point


  Verbs:
      cd
      exit
      help
      set
      show
      version

->
```

Figure 63. REMOTESAP2 Target

5.5.15 Account

The account target represents user accounts. It does not contain any targets.

5.5.15.1   Supported Properties

The supported properties of the target account are as follows:

Property	Task
userid	This read only property defines the unique id for each user.
username	This property gives the usermname of a particular account. This is settable except for userid=1. Username Length must be more than 1 character and less than 16 characters. ->set username=sdf
pmilanprivileges	This property gives the ipmi lan privileges. It can be set except for userid=1. Only numbers are allowed. ->set ipmilanprivileges=4
password	This property gives the password of a particular user. It can be set xcept for userid=1; password length should be less than 16 characters. ->set password=ssd
enabledstate	This property shows the state of the user. This property is settable except for userid=1. Use 0 for disable and 1 for enable. For example to enable the user set the value of this property to 1 ->set userid=1 For example to enable the user set the value of this property to 1 ->set userid=1
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.15.2　Supported Verbs

The supported verbs of the account target are as follows:

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
delete	Delete. To delete, go to sp1 target and delete account (n) where n>2.
set	Set the r/w supported properties
show	Show all the targets, properties, and verbs supported by this target.
version	Show the current version of SMASH*.

```
->cd account1
COMMAND COMPLETED :
cd account1

 ufip=/system1/sp1/account1

->show
COMMAND COMPLETED :
show

 ufip=/system1/sp1/account1
  Properties:
       userid=1
       username=anonymous
       ipmilanprivileges=4
       password=[INVISIBLE]
       enabledstate=User is enabled
       identity=user account


  Verbs:
       cd
       delete
       exit
       help
       set
       show
       version

->
```

Figure 64. ACCOUNT1 Target

5.5.16   Logs1

The logs target is the containing target for log records of the ipmi sel. The System Event Log is a non-volatile repository for system events and certain system configuration information. This target contains all the read only properties. It contains log records as the targets.

5.5.16.1   Supported Properties

The supported properties of the target Logs1 as follows.

Property	Task
MaxNumberOfRecords	This read only property gives information about maximum number of log records.
Description	A read only description about the target.
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.16.2   Supported Verbs

The supported verbs of the Logs1 target are as follows:

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
delete	Delete. To delete, go to sp1 target and delete account(n) where n>2.

Verb	Is used to
show	Show all the targets, properties, and verbs supported by this target.
version	Show the current version of SMASH*.

```
->show
COMMAND COMPLETED :
show

 ufip=/system1/sp1/logs1
  Targets:

        record10/
        record11/
        record12/
        record13/
        record1/
        record2/
        record3/
        record4/
        record5/
        record6/
        record7/
        record8/
        record9/

    Properties:
        MaxNumberOfRecords=3639
        CurrentNumberOfRecords=13
        Description=IPMI SEL
        identity=IPMI SEL


    Verbs:
        cd
        delete
        exit
        help
        show
        version

```

Figure 65. LOGS1 Target

5.5.17   Record

The record target represents the individual SEL entries. SEL records are in a list. Each SEL entity is a record. This does not have any targets.

5.5.17.1   Supported Properties

The supported properties of the target Record1 are as follows:

Property	Task
LogCreationClassName	This read only property gives information about the log creation class name.
logname	This read only property gives the name of the log record
CreationClassName	This read only property gives the creation class name of the record
RecordID	SEL Entries have a unique 'Record ID' field. This is the unique ID for the particular record. This is a read only property.
MessageTimeStamp	This read only property gives the time stamp of the record creation
RecordData	The record data field that is passed in the request consists of all bytes of the

Property	Task
	SEL event record. This property gives information of the record and is read only.
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.17.2   Supported Verbs

The supported verbs of the Record target are as follows:

Verb	Is used to
cd	Change from one valid target path to any other valid target path.
exit	Exit from the current SMASH* session.
help	Provide information on using SMASH*.
show	Show all the targets, properties, and verbs supported by this target.
version	Show the current version of SMASH*.

```
->show
COMMAND COMPLETED :
show

 ufip=/system1/sensor2
  Properties:
       Description=MDS-voltage33SBV(1.0.32):CIM Voltage for system1
       systemCreationClassName=CIM_ComputerSystem
       CurrentReading=3.32
       BaseUnits=Volts
       SystemName=system1
       CreationClassName=CIM_Sensor
       DeviceID=1.0.32
       Name=MDS-voltage33SBV(1.0.32)
       SensorType=CIM Voltage
       HealthState=Not Defined
       OperationalStatus=Not Defined
       identity=MDS-voltage33SBV(1.0.32):CIM Voltage for system1


  Verbs:
       cd
       exit
       help
       show
       version


->
```

Figure 66. RECORD1 Target

5.5.18 Sensor

A typical server BMC would provide sensors for baseboard temperature, voltage, and chassis intrusion monitoring. A sensor uses one type of energy, a signal of some sort, and converts it into a reading for the purpose of information transfer. The sensor doesn't have any targets. All properties of this target are read only properties.

5.5.18.1   Supported Properties

Property	Task
Description	This read only property describes the sensor and the target under which it is present.
SystemCreationClassName	This read only property gives the system creation class name and is a read only property.
CurrentReading	This read only property gives the current reading shown by the sensor
BaseUnits	This read only property gives the units for the value given by current reading property.
SystemName	This read only property gives the target name under which this sensor exists
CreationClassName	This read only property gives the creation class name of the sensor.
DeviceID	This read only property gives the device ID.
Name	This read only property gives the name of the current sensor.
SensorType	This read only property gives the type of sensor.
HealthState	This read only property gives the health status of the sensor.
OperationalStatus	This read only property defines the operational status of the sensor.
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

5.5.18.2   Supported Verbs

The supported verbs of the sensor target are as follows:

Verb	Is used to
Cd	change from one valid target path to any other valid target path.
Exit	exit from the current SMASH* session.
Help	provide information on using SMASH*.
show	show all the targets, properties, and verbs supported by this target.
version	show the current version of SMASH*.

```
->show
COMMAND COMPLETED :
show

 ufip=/system1/sensor2
  Properties:
        Description=MDS-voltage33SBV(1.0.32):CIM Voltage for system1
        systemCreationClassName=CIM_ComputerSystem
        CurrentReading=3.32
        BaseUnits=Volts
        SystemName=system1
        CreationClassName=CIM_Sensor
        DeviceID=1.0.32
        Name=MDS-voltage33SBV(1.0.32)
        SensorType=CIM Voltage
        HealthState=Not Defined
        OperationalStatus=Not Defined
        identity=MDS-voltage33SBV(1.0.32):CIM Voltage for system1


  Verbs:
        cd
        exit
        help
        show
        version


->
```

Figure 67. SENSOR2 Target

5.5.19 Creating Targets

Dynamic targets in SMASH*(without CIM) are the sensors and their associated entities. You need to go through the sdr and search for Full and Compact record types. Name the Full type as numsensor<index> (indicates the analog sensors) and the Compact type as the sensor<index> (indicates the discrete sensors). While a sensor instance is discovered, the EntityID and the EntityInstance of the record are also seen. EntityID denotes the entity the sensor is monitoring. If the EntityID is of type cpu and Entityinstance is 1, then the parent of sensor1 will be cpu1. Other sensor related entity instances are created in a similar manner.

```
                        >> SMASH-CLP Console v1.09 <<
->show
COMMAND COMPLETED :
show

 ufip=/
  Targets:

        settings1/
        system1/

  Properties:
        identity=root


  Verbs:
        cd
        exit
        help
        show
        version


->
```

Figure 68. SMASH* Target

Glossary

Term	Definition
ACPI	Advanced Configuration and Power Interface
ARP	Address Resolution Protocol
BMC	Baseboard management controller
CLI	Command-line interface
DHCP	Dynamic Host Configuration Protocol
DMTF	Distributed Management Task Force
FRU	Field replaceable unit
HSBP	Hot-swap backplane
HSC	Hot-swap controller
OFU	Intel® One Boot Flash Update utility
IDA	Intel® Deployment Assistant
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
KVM	Keyboard, video, mouse
LAN	Local area network
MAC	Media Access Control
WinPE	Microsoft Windows* Preinstallation Environment
NIC	Network interface card
OOB	Out-of-band
OEM	Original equipment manufacturer
PEF	Platform event filtering
PET	Platform Event Trap
PSMI	Power Supply Management Interface
SDR	Sensor Data Record
SEL	System Event Log
SMTP	Simple Mail Transport Protocol
SMASH	Systems Management Architecture for Server Hardware
SM CLP	SMASH Command Line Protocol
SMS	Server management software
SNMP	Simple Network Management Protocol
SOL	Serial-over-LAN
WS-MAN	Web Services for Management