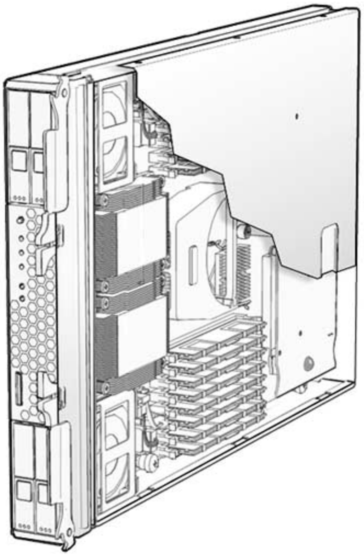
Sun Blade X6250 Server Module Embedded Lights Out Manager Administration Guide



Sun Microsystems, Inc.
www.sun.com

Part No. 820-1253-14
June 2008, Revision A

Submit comments about this document at: `http://www.sun.com/hwdocs/feedback`

Contents

Figures

Preface

The *Sun Blade X6250 Server Module Embedded Lights Out Manager Administration Guide* provides instructions for managing Sun servers using the Sun Blade X6250 server module's service processor and the Embedded Lights Out Manager (ELOM).

How This Document Is Organized

Chapter 1 provides an overview of the ELOM, and indicates tasks and system management tasks.

Chapter 2 details the various ways to connect to and communicate with your server module.

Chapter 3 describes how to use the ELOM's web GUI to monitor your server.

Chapter 4 provides information about using the browser interface to manage and maintain the server module.

Chapter 5 describes how to use the remote console through a browser.

Chapter 6 details an alternative method of managing your server using the command-line interface (CLI).

Chapter 7 describes how to use the Intelligent Platform Management Interface (IPMI), independent of the operating system, to manage field replaceable units (FRUs) and monitor the health of your system.

Chapter 8 helps you understand the basics of the Simple Network Management Protocol (SNMP).

Appendix A gives you a quick reference to the commands you can use with Embedded Lights Out Manager.

Glossary provides definitions for a list of technical words and phrases.

Using UNIX Commands

This document might not contain information about basic UNIX® commands and procedures such as shutting down the system, booting the system, and configuring devices. Refer to the following for this information:

- Software documentation that you received with your system
- Solaris™ Operating System documentation, which is at `http://docs.sun.com.`

Typographic Conventions

Typeface*	Meaning	Examples
`AaBbCc123`	The names of commands, files, and directories; onscreen computer output.	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail.`

`AaBbCc123`	What you type, when contrasted with onscreen computer output.	`%` **`su`**
		`Password:`

AaBbCc123	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the *User's Guide.* These are called *class* options. You *must* be a superuser to do this. To delete a file, enter `rm` *filename*.

* The settings on your browser might differ from these settings.

Related Documentation

For the most up-to-date information about the Sun Blade X6250 server module, navigate to your blade server at:

http://docs.sun.com/app/docs/prod/blade.x6250.

After the product's world-wide release date, translated versions of some of these documents are available at:

http://docs.sun.com.

Select a language from the drop-down list, and navigate to the Sun Blade X6250 Server Module document collection using the Blade Servers category link. Available translations for the Sun Blade X6250 server module include Simplified Chinese, Traditional Chinese, French, Japanese, and Korean

The English documentation is revised more frequently. Therefore it might be more up-to-date than the translated documentation.

Sun Support, and Training

Sun Function	URL
Support	http://www.sun.com/support/
Training	http://www.sun.com/training/

Third-Party Web Sites

Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

Sun is interested in improving its documentation. We welcome your comments and suggestions. Submit your comments at:

http://www.sun.com/hwdocs/feedback.

Please include the following title and part number of this document with your feedback:

Sun Blade X6250 Server Module Embedded Lights Out Manager Administration Guide, 820-1253-14

CHAPTER 1

Sun Blade X6250 Server Module ELOM Overview

This chapter serves as an overview to the Sun Blade X6250 server module's Embedded Lights Out Manager (ELOM).

ELOM Features

The ELOM provides a dedicated system of hardware and supporting software that enables you to manage your Sun server independently of the operating system and through several interfaces. The following sections describe some of the features of the Sun Blade X6250 server module service processor's ELOM:

- "Embedded Lights Out Manager Common Tasks" on page 2
- "Sun Blade X6250 Server Module Default Settings" on page 3
- "About the Preconfigured Administrator Account" on page 3
- "Locator LED for Server Module" on page 3
- "Responding to LED Indicators" on page 4

Embedded Lights Out Manager Common Tasks

The following table shows common tasks and the management interfaces used to perform each task.

TABLE 1-1 Common Tasks

Task	IPMI	Web GUI	CLI	SNMP
Redirect the system graphical console to a remote client browser.	-	Yes	-	-
Connect a remote drive to the system as a virtual drive.	-	Yes	-	-
Connect a remote CD-ROM drive to the system as a virtual CD-ROM drive.	-	Yes	-	-
Monitor system fans, temperatures, and voltages remotely.	Yes	Yes	Yes	Yes
Monitor system BIOS messages remotely.	Yes	Yes	Yes	-
Monitor system operating system messages remotely.	Yes	Yes	Yes	-
Interrogate system components for their IDs and serial numbers.	Yes	-	Yes	Yes
Redirect the system serial console to a remote client.	Yes	-	Yes	-
Monitor system status (health check) remotely.	Yes	Yes	Yes	Yes
Interrogate system network interface cards remotely for MAC addresses.	Yes	Yes	Yes	-
Manage user accounts remotely.	Yes	Yes	Yes	-
Manage system power status remotely (power on, power off, power reset).	Yes	Yes	Yes	-
Monitor and manage environmental settings for key system components (CPUs, motherboards, and fans).	Yes	Yes	Yes	Monitor only

Sun Blade X6250 Server Module Default Settings

Sun has configured the SP controller and SP firmware on your server to reflect the most common default settings used in the field. It is unlikely that you will need to change any of these defaults.

TABLE 1-2 Default Settings

System Component	Default Status	Action Required
Service Processor card	Preinstalled	None
Service Processor firmware	Preinstalled	None
IPMI interface	Enabled	None
Web-based interface	Enabled	None
Command-line interface (CLI)	Enabled	None
SNMP interface	Enabled	None

About the Preconfigured Administrator Account

The ELOM is shipped with one preconfigured administrator account:

User name: **root**
Password: **changeme**

The preconfigured administrator account, known as root, cannot be deleted. You can only change the account password. The root account offers built-in administrative privileges (read and write access) to all service processor features and commands. To increase security, change the default password to a new, unique password. See Chapter 5 for details.

Note – The Chassis Manager Module (CMM) Integrated Lights Out Manager (ILOM) is shipped with an identical preconfigured administrator account, with user name `root` and the default password set to `changeme`.

Locator LED for Server Module

The Locator LED (also called the system indicator LED) is a small light on the front panel. Use the LED to help you locate the server module from among many other server modules in a chassis in a data center.

Responding to LED Indicators

The front panel of your Sun Blade X6250 server module has a Fault Indicator LED. You can use the state of the Fault Indicator LED to determine the status of your server. For normal server operation, the LED is off (not lit). A solidly lit amber LED indicates critical error, and a blinking LED indicates a warning. Use the ELOM to troubleshoot the system when the Fault Indicator LED is blinking (see "Managing the System Indicator and Fault LED" on page 35).

1. **If the amber LED on the front panel is solidly lit, power off the server module, and remove it from the chassis or rack.**

Caution – To remove the server module from the chassis, follow the procedures detailed in the *Sun Blade X6250 Server Module Service Manual*.

---

2. **Open the unit, and locate the two blue or red push buttons.**

   One of these, when pressed, will light up the LED failure indicators next to any defunct Dual Inline Memory Module (DIMM).

   Similarly if one of the two CPUs in the Sun Blade X6250 server module is triggering the front panel Fault Indicator LED, then the indicator next to the defunct CPU will light up.

For instructions and cautions concerning handling and servicing the Sun Blade X6250 server module hardware, refer to the *Sun Blade X6250 Server Module Service Manual*.

CHAPTER 2

Connecting to the ELOM

This chapter details the ways to connect and communicate with your Sun Blade X6250 server module.

Note – You must have already installed your server and determined the IP address of the service processor. Information about installing the server and determining the IP address of the service processor is available in the *Sun Blade X6250 Server Module Installation Guide.*

Connection Methods

There are two ways to connect to the Embedded Lights Out Manager (ELOM) in your server:

- "Connecting Using Ethernet" on page 5
- "Connecting Through the Chassis Manager Module" on page 7

Connecting Using Ethernet

Ethernet connectivity provides full access to both the ELOM command-line interface (CLI) and the ELOM web GUI. Both options allow you to manage and maintain the server. This section contains the following two connection procedures:

- Connecting to the CLI using Ethernet "To Connect to the CLI" on page 6.
- Connecting to the web GUI using Ethernet "To Connect to the Web GUI" on page 6.

Note – You will need the IP address of your ELOM, which you obtained during the setup and installation of your server module (see the *Sun Blade X6250 Server Module Installation Guide).*

▼ To Connect to the CLI

Be sure that you have connected a LAN to the NET MGT 0 port on the chassis.

1. **Start your SSH client.**

   When you first access the CLI, you will need to use the preconfigured user name and password:

   - Default user name – **`root`**
   - Default password – **`changeme`**

2. **To log in to the ELOM, enter the following command:**

   $ **`ssh`** *username*`@`*ipaddress*

   username An account user name.
   ipaddress The IP address of the ELOM.

   A password prompt appears.

3. **When prompted, enter the password.**

   The CLI prompt appears:

   –>

   For information about managing the server using the CLI, see Chapter 6.

To Log out of the CLI:

- **To log out of the CLI, enter the following command:**

  –> **`exit`**

▼ To Connect to the Web GUI

Be sure that you have connected a LAN to the NET MGT 0 port on the chassis.

1. **To log in to the web GUI, enter the IP address of the ELOM into your browser.**

   The login screen appears.

2. **Enter your user name and password.**

   When you first access the web GUI, it prompts you for the default user name and password:

- Default user name – **`root`**
- Default password – **`changeme`**

The default user name and password are in lowercase characters.

3. **Click Log In.**

   Chapter 3 shows how to use the web GUI.

To Log Out of the Web GUI:

● **Click Log Out at the top right of the web GUI screen.**

The login screen appears.

Connecting Through the Chassis Manager Module

The chassis serial connector connects to the Chassis Management Module's (CMM) Integrated Lights Out Manager (ILOM). You can connect to the server module ELOM via this serial connection using a RJ-45 cable and a terminal (or a PC running terminal emulation software). Once connected, you can use the command-line interface (CLI) to manage, maintain, and configure the server.

▼ To Connect Through the Chassis Manager Module

1. **Verify that your terminal, laptop, or terminal server is operational.**
2. **Configure the terminal device or the terminal emulation software to use the following settings:**
   - 8,N,1 (eight data bits, no parity, one stop bit)
   - 9600 baud (default, can be set to any standard rate up to 57600)
   - Disable software flow control (XON/XOFF)
3. **Connect a serial cable from the serial port on the CMM to the terminal device.**

   Refer to the chassis documentation for the location of the chassis serial port.

4. **Press Enter on the terminal device.**

   This action establishes the connection between the terminal device and the CMM ILOM.

   The CMM ILOM displays its login prompt:

   ```
   SUNCMMnnnnnnnnnn login:
   ```

   The first string in the prompt is the default host name. It consists of the prefix SUNCMM and the CMM ILOM's MAC address. The MAC address for each service processor is unique.

5. **Log in to the CLI:**

   When you first access the CLI, you will need to use the preconfigured user name and password:

   - Default user name – **`root`**
   - Default password – **`changeme`**

   Once you have successfully logged in, the CMM ILOM displays its default command prompt:

   ```
   ->
   ```

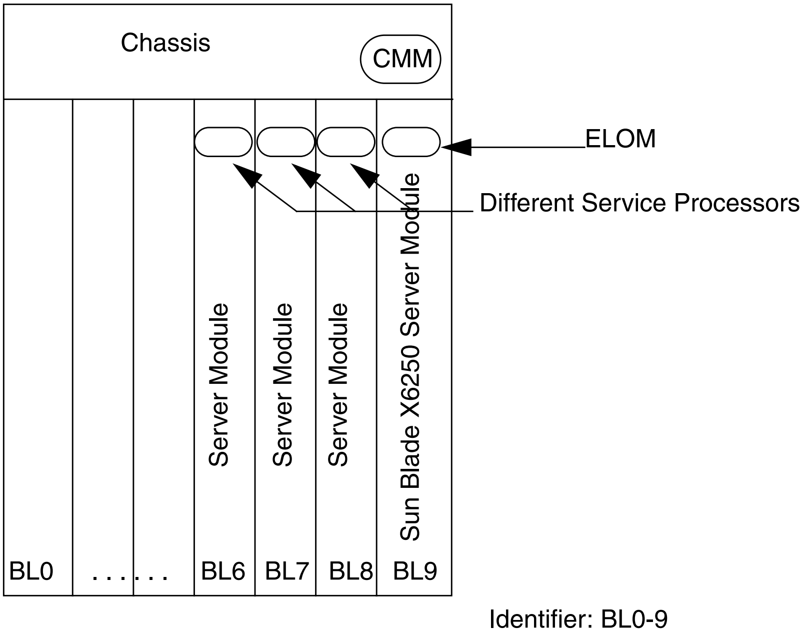
   You are now connected to the CMM ILOM CLI.

6. **Navigate to the server module ELOM by entering this command:**

   ```
   cd /CH/BLn/SP/cli
   ```

   n The position number of the server module in the chassis. Use FIGURE 2-1 to assist you in determining the server module number, and to understand the relationship between the CMM and different server module service processors.

FIGURE 2-1 Chassis and Server Module ELOM Address Identifiers



7. **Enter the command `start`.**

   The following prompt appears:

```
Enter Y to continue or N to cancel.
```

8. **Enter `Y` to continue.**

   If you enter **`N`**, the server module will return you to the CMM CLI prompt.

9. **Enter the password when prompted.**

   Supply the password for root. The preconfigured default is **`changeme`**.

   The server module ELOM prompt appears.
   For information about managing and maintaining the server module, see Chapter 6.

10. **When you are finished, enter `exit` at the ELOM CLI prompt.**

    The CMM CLI prompt appears.

The following display shows an example of the login screen:

```
 -> cd /CH/BL2/SP/cli
/CH/BL2/SP/cli

-> start
Are you sure you want to start /CH/BL2/SP/cli (y/n)? y
Password:          Enter the password to the server module ILOM.

Sun(TM) Integrated Lights Out Manager

Version N.N

Copyright 2006 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.

Warning: password is set to factory default.

-> exit            Enter this command to exit the server module ILOM
                     and return to the CMM ILOM.
Connection to 10.6.122.33 closed.
```

CHAPTER 3

Monitoring the Server System Using the Web GUI

This chapter provides information about how to use the web GUI and the Sun Blade X6250 server module software to monitor your server.

It includes the following sections:

Using the Web GUI

The web GUI allows you monitor and manage local and remote systems, using a standard browser.

You can also monitor the server remotely by redirecting the server's console to a remote workstation or laptop. This requires configuring the remote system's keyboard and mouse to act as the server's keyboard and mouse. You can configure the diskette drive or CD-ROM drive on the remote system as if it were connected to the Sun server. You can also redirect diskette images (`.img`) and CD-ROM images (`.is`) for remote access. Remote configuration issues are covered in Chapter 5.

Browser and Software Requirements

The web GUI has been tested successfully with recently released Mozilla™ Firefox, and Internet Explorer browsers, and may be compatible with other browsers.

The ELOM product is preinstalled on the Sun server. However, you need Java™ software on the client to perform redirection as described in Chapter 10.

Users and Permissions

After you log in to the web GUI, you can perform management, basic software tasks, Intelligent Platform Management Interface (IPMI) tasks, and system monitoring.

ELOM permissions for user accounts define user limitations. For example:

administrator – Enables full (unlimited) read and write access to all ELOM software features, functions, and commands.

operator – Enables read-only access to a limited number of ELOM software features, functions, and commands, plus management access to Indicator and Fault LEDs.

user and **callback**– Enables read-only access to a limited number of ELOM software features, functions, and commands.

For more information about user accounts, including setting permissions and changing passwords using the web GUI, see "Managing User Accounts" on page 31.

Web GUI Tasks

Some of the common tasks you can perform using the web GUI include:

Configure connection methods:

- Connect a remote diskette drive or diskette image to the system as a virtual diskette drive.
- Connect a remote CD-ROM drive or CD-ROM image to the system as a local or virtual CD-ROM drive.
- Redirect the system's graphical console to a remote client browser.

Monitor and manage system status

- Monitor the status of system fans, temperatures, and voltages remotely.
- Monitor BIOS power-on self-test (POST) progress log entries remotely.
- View, save, and clear system event logs.

- Examine component information, including CPUs, DIMMs, and network interface cards (NIC).
- Power on, power off, power cycle, and reset the system remotely.

Manage and modify system variables

- Manage user accounts locally and remotely.
- Configure settings.
- Update BIOS firmware.

Accessing the System Using a Browser

The ELOM boots automatically when the server module is inserted into a powered chassis. This usually occurs within one minute. However, if the management Ethernet is not connected, or if the ELOM's Dynamic Host Configuration Protocol (DHCP) process fails due to the absence of a DHCP server on the management network, the ELOM might take a few minutes longer to boot.

Note – Disabling the use of the browser proxy server (if one is used) for access to the management network might speed up the response time.

▼ To Access the System Using a Browser

1. **To access the web GUI, enter the IP address of the ELOM in your browser.**

   The login screen appears.

2. **Type a user name and password.**

   To configure and manage the server use a user account with administrator privileges.

3. **Click Log In.**

   The main menu screen appears.

To log out of the web GUI:

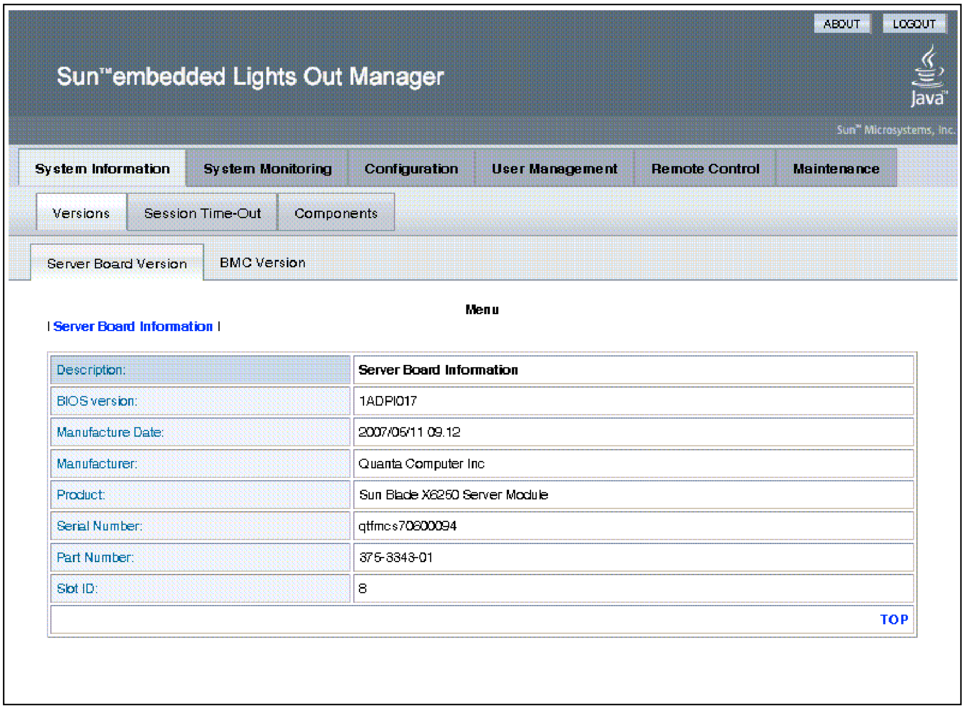
- **Click the Log Out button.**

  The Log Out button is located at the top right of the interface screen.

Viewing the System From the Web GUI

Your server is equipped with a number of sensors that measure component voltages, temperatures, and fan speed. The System Information tab reflects the current system status.

FIGURE 3-1 ELOM System Information Screen



Description:	Server Board Information
BIOS version:	1ADPI017
Manufacture Date:	2007/05/11 09.12
Manufacturer:	Quanta Computer Inc
Product:	Sun Blade X6250 Server Module
Serial Number:	qtfmcs70600094
Part Number:	375-3343-01
Slot ID:	8

The menu items on the tabs are listed in TABLE 3-1:

TABLE 3-1 ELOM Tab Detail Choices

Main Tab	Sub-level Tab	Where to Find Details
System Information		"Viewing System Information" on page 16
	Versions	"Viewing System Information" on page 16
	Session Time-Out	"Setting Session Timeout" on page 44
	Components	"Viewing Component Information" on page 18

TABLE 3-1 ELOM Tab Detail Choices *(Continued)*

Main Tab	Sub-level Tab	Where to Find Details
System Monitoring		
	Sensor Reading	"Monitoring the System" on page 19
	Event Logs	"Viewing and Managing the Event Log" on page 22
	System Indicator	To view location of interior LEDs, refer to your service manual To change, refer to: "Managing the System Indicator and Fault LED" on page 35
	Fault LED	Refer to your service manual
Configuration		
	Network	"To View NIC Information" on page 19
	Email Notification	"Configuring Email Notification" on page 27
	Platform Event Filter	"Configuring Platform Event Filters" on page 27
	Set Time	"Setting the Time" on page 44
	SSL Certificate	"Configuring the SSL Certificate" on page 28
	ADS Configuration	"Configuring ADS" on page 29
	SNMP	"Recovering from a Corrupt Service Processor" on page 42
User Management		
	Add User	"To Add a User" on page 33
Remote Control		"Starting the Remote Console Application" on page 48
	Redirection	"Redirecting Keyboard, Video, Mouse, or Storage Devices" on page 49
	Remote Power Control	"Controlling Server Power" on page 36
	Hotkey Setup	Chapter 5
Maintenance		
	Firmware Upgrade	"Updating the Firmware" on page 38
	Reset BMC	"Resetting the BMC/SP" on page 36

The following section describes how to monitor the server using the browser and the ELOM software.

Viewing System Information

The System Information tab provides information about server board and system components, such as the service processor (SP), the CPU, the memory, and the network interface cards (NIC). Details are found in the Versions and Components submenu tabs.

Note – The service processor (SP) is also referred to as the BMC. Wherever BMC is mentioned, consider it different terminology for the SP.

▼ To View System Information

- **On the main menu, click the System Information tab.**

  The System Information submenu appears, allowing you to view the Versions, Session Time-Out, and Components submenu tabs.

Viewing Version Information

▼ To View Server Board Version Information

- **From the Versions submenu, select the Server Board Version tab.**

  The Server Board Version screen appears. It displays information about the server board installed in the system, and presents the information in a tabular format. For example:

TABLE 3-2 Sample Server Board Information

Description	Server Board Information
BIOS Version:	1ADP1017
Manufacture Date:	2007/05/11 09:12
Manufacturer:	Quanta Computer, Inc.

TABLE 3-2 Sample Server Board Information *(Continued)*

Description	**Server Board Information**
Product:	Sun Blade X6250 Server Module
Serial Number:	qtfmcs7060094
Part Number:	375-3343-01
Slot ID:	8

▼ To View BMC Version Information

- **From the Versions submenu, select the BMC Version tab.**

  The BMC Version screen appears. It displays information about the BMC installed in the system, and presents the information in a tabular format. For example:

TABLE 3-3 Sample BMC Version Screen

Description	BMC Board Information
Device ID	5
Device Revision	0
Firmware Revision	4.0.26
IPMI Revision	2.0
CPLD version	140

Viewing Component Information

▼ To View CPU Information

- **From the System Information menu, click the Components submenu tab, and then select CPU.**

  The CPU information screen appears. The CPU information is presented in a tabular format (see TABLE 3-4). A separate table of information is available for each of the server's CPU, regardless if a CPU is installed or not.

TABLE 3-4 Sample CPU Information

Description:	CPU Information
CPU	0
Status:	Enable
Socket:	CPU0
Manufacturer:	Intel
Model:	Xeon 5300
Frequency:	1866MHz

▼ To View Memory Information

- **From the System Information menu, click the Components submenu tab, and then select Memory.**

  The Memory submenu screen appears. It displays information about each of the DIMMs installed in your server. The CPU information is presented in a tabular format (see TABLE 3-5).

TABLE 3-5 Sample Memory Information

Description	Memory Information
Memory Module	1
Status:	Ok
Socket:	DIMM_A0

TABLE 3-5 Sample Memory Information *(Continued)*

Description	Memory Information
Module Size:	2048MB
Type:	FBDIMM
Frequency	533MHz

▼ To View NIC Information

- **From the System Information menu, click the Components submenu tab, and then select NIC.**

  The NIC submenu screen appears. It displays information about the network interface card installed in your server. The NIC information is presented in a tabular format (see TABLE 3-6).

TABLE 3-6 Sample of NIC Information

Description:	Network Interface Card 0 Information
Manufacturer:	Intel
Product Name:	ESB Dual Port Gb Ethernet NIC
Product Part Number:	6312
Product Serial Number:	00:16:36:F1:67:34
Port Number:	02
MAC Address 1:	00:16:36:F1:67:34
MAC Address 2:	00:16:36:F1:67:34

Monitoring the System

Sensors placed throughout the system provide information about the state of critical server hardware. The sensors allow the system to monitor temperature, voltage, and operational status. Using the System Monitoring submenu screens you can view the these sensors, and monitor the health of your server’s critical components. For example, you can check the temperature of each CPU and the voltage level of the system’s DC voltage lines. The System Monitoring submenu screens also allow you to view and manage the system log, the System Indicator LED, and the Fault LED. For information about the System Indicator LED and the Fault LED, see Chapter 4.

▼ To Monitor the System

- **On the main menu, click System Monitoring.**

  The System Monitoring submenu appears, allowing you to view the Sensor Reading, Event Logs, System Indicator, and Fault LED tabs.

Reading Sensors

The Sensor Reading Tab provides access to the Sensor Summary, the Temperature, Voltage, and Chassis Status screens.

▼ To Read Sensors

- **From the System Monitoring tab, click the Sensor Reading Tab.**

  The Sensor Reading tab allows you to select the Summary, Temperature, Voltage, and Chassis Status tabs.

▼ To View a Sensor Summary

- **From the Sensor Reading submenu tab, select the Summary tab.**

  The Summary screen appears. It provides an overview of the status of the system sensors. The screen provides the status of the Fault LED, the server’s power status, the temperature status of all critical components, and the status of each of the monitored voltage lines.

▼ To Monitor Temperatures

- **From the Sensor Reading submenu tab, select the Temperature tab.**

  The Temperature screen appears. It provides the status, the actual temperature, and the upper critical and non-critical temperature thresholds for each system-critical component. The Temperature submenu screen displays the information in a tabular format. It provides a separate table for each component. TABLE 3-7 shows a sample of the temperature monitoring readings for CPU 0.

TABLE 3-7 Sample Temperature Monitor Readings

Description:	CPU Temp
Upper noncritical threshold is readable:	93.0
Upper critical threshold is readable:	95.0
Sensor Reading:	54.0
Status:	ok

A similar panel is repeated for each monitored entity.

▼ To Monitor Voltages

- **From the Sensor Reading submenu, select the Voltage tab.**

  The Voltage screen appears. It provides the status, the actual voltage reading, and the upper critical and non-critical voltage thresholds for each of the monitored voltage lines. The Voltage submenu screen displays this information in a tabular format. TABLE 3-8 shows a sample of this information for P_VCCP0.

TABLE 3-8 Sample of Voltage Information

Description	P_VCCP0
Lower non-critical threshold is readable:	0.000
Lower critical threshold is readable:	0.000
Upper non-critical threshold is readable:	1.342
Upper critical threshold is readable:	1.342
SensorReading:	1.147
Status:	ok

▼ To Monitor the Chassis Status

- **From the Sensor Reading submenu, select the Chassis Status tab.**

  The Chassis Status submenu screen appears. The Chassis Status screen shows the actual senor readings for the critical components of the chassis in to which you have installed your Sun Blade X6250 server module. These critical components include the chassis fans (represented in RPM), the voltage and amperage for the chassis power supplies, and the ambient chassis temperatures. The information is presented a tabular format showing the name, the reading, and the unit of measurement.

Viewing and Managing the Event Log

The Event Log screen allows you to view and manage the System Event Log (SEL). The SEL is a record of event occurrences. To record events in the SEL, you must have previously determined which events require logging. See "Configuring Platform Event Filters" on page 27.

▼ To View and Manage the Event Log

- **From the System Monitoring tab on the main menu, click the Event Logs submenu tab.**

  The Event Logs submenu screen appears. The View Event Logs, Save Event Logs, and Clear Event Logs submenus become available.

▼ To View the Event Logs

- **From the Event Logs submenu, select View Event Logs.**

  The system event log appears. Each entry in the log represents an action that occurred on the system. The system lists each action, rating the action's severity, providing time-stamp, and describing the event. The information is presented in a tabular format.

▼ To Save the Event Log

You may want to save the event log for administrative or diagnostic purposes.

1. **From the Event Logs submenu, click the Save Event Logs tab.**

   The Save Event Log screen appears.

2. **Click the Save Event Log button to prompt the browser to ask you where to save a copy of the event log.**

▼ To Clear the Event Log

The Event Log may need to be cleared to signify a fresh procedure, or to identify system performance under load.

1. **From the Event Log menu, choose Clear Event Log.**

2. **Click the Clear Event Log button to start a fresh event log.**

CHAPTER 4

Configuring, Managing, and Maintaining the Server Using the Web GUI

This chapter provides information about how to use the web GUI and the Sun Blade X6250 server module software to configure, manage, and maintain your server.

This chapter is divided into the following sections:

- "Configuring the System" on page 25
- "Managing the System" on page 31
- "Managing and Maintaining the Server" on page 34

This chapter addresses your local system. For information about how to redirect your commands to a remote system, see Chapter 5.

For information about connecting to the ELOM see Chapter 2.

Configuring the System

The Configuration submenu tabs allow you to configure the operation of the server. This section contains the following server configuration procedures:

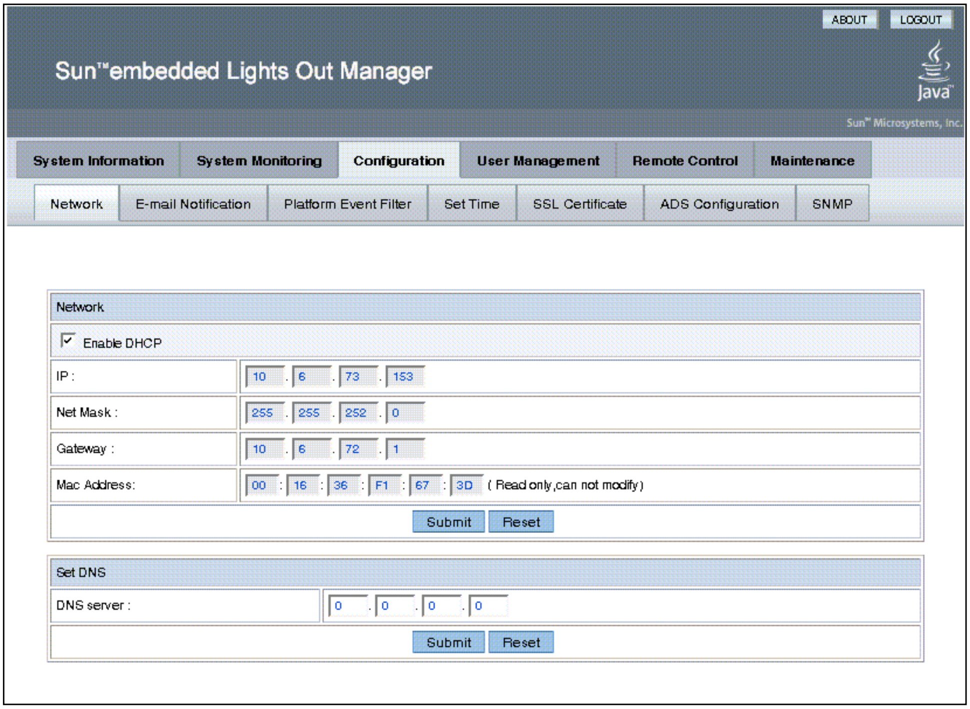
- "Configuring Email Notification" on page 27
- "Configuring Platform Event Filters" on page 27
- "Configuring the SSL Certificate" on page 28
- "Configuring ADS" on page 29
- "Configuring SNMP" on page 30

▼ To Configure the Server

- **On the ELOM main menu, click the Configuration tab.**

  The Configuration submenu tabs appear (see FIGURE 4-1). You are now able to access the Network, E-mail Notification, Platform Event Filter, Set Time, SSL Certificate, ADS Configuration, and SNMP tabs.

FIGURE 4-1 The Configuration submenu Tabs



Network

☑ Enable DHCP

IP :	10 . 6 . 73 . 153
Net Mask :	255 . 255 . 252 . 0
Gateway :	10 . 6 . 72 . 1
Mac Address:	00 : 16 : 36 : F1 : 67 : 3D (Read only,can not modify)

Set DNS

DNS server :	0 . 0 . 0 . 0

▼ To Configure Network Settings

- **From the Configuration submenu, click the Network tab.**

  The Network configuration screen appears (see FIGURE 4-1). Use this screen to enable or disable DHCP and set DNS. If you disable DHCP, you must manually supply the IP address, the anatomist, and the gateway.

Note – The MAC address is hardware encoded and unique to each system. It cannot be modified.

Configuring Email Notification

The E-mail Notification screen enables you to configure the email recipients for any ELOM generated events. The system allows you to designate up to 10 recipients. Email notification is used in conjunction with Platform Event Filters (PEF). PEFs are event traps that allow you to associate an action, or a set of actions, with the occurrence of a specific event. One such action is mail notification. The Send Mail action is enabled in the Platform Event Filter screen, and configured in the E-mail Notification screen.

▼ To Configure Email Notification

- **From the Configuration submenu, click the E-mail Notification tab.**

  The Enable E-mail Notification screen appears. You must supply the name of the SMTP server and the Sender, and designate the receiver email addresses.

Configuring Platform Event Filters

▼ To Configure Platform Event Filters

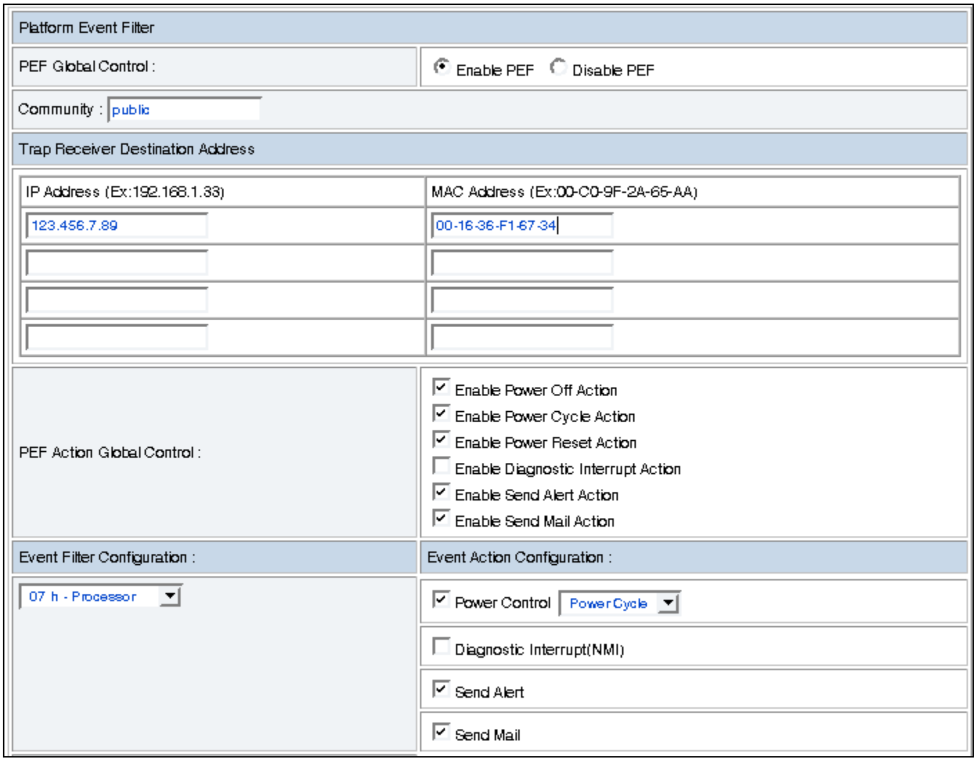
1. **From the Configuration submenu, click the Platform Event Filter tab.**

   The Platform Event Filter screen appears (see FIGURE 4-2). The Platform Event Filter screen is composed of three sections, the PEF Global Control section, Trap Receiver Destination Address section, and Event Filter Configuration section.

   Use the Platform Event Filter section to enable PEF and designate the SNMP community. Use the Trap Receiver Destination Address section to list the IP and MAC addresses for the trap receiver, and use this section to enable the PEF actions. Use the Event Filter Configuration section to configure up to six event filters. You must select the sensors to trap (from the drop-down list) and the resultant action (using the action check boxes).

2. **Click Submit to save your configuration.**

FIGURE 4-2 The Platform Event Filter Screen Detail



Platform Event Filter

PEF Global Control : ● Enable PEF ○ Disable PEF

Community : public

Trap Receiver Destination Address

IP Address (Ex:192.168.1.33)	MAC Address (Ex:00-C0-9F-2A-65-AA)
123.456.7.89	00-16-36-F1-67-34

PEF Action Global Control :

- ☑ Enable Power Off Action
- ☑ Enable Power Cycle Action
- ☑ Enable Power Reset Action
- □ Enable Diagnostic Interrupt Action
- ☑ Enable Send Alert Action
- ☑ Enable Send Mail Action

Event Filter Configuration : 07 h - Processor

Event Action Configuration :

- ☑ Power Control: Power Cycle
- □ Diagnostic Interrupt(NMI)
- ☑ Send Alert
- ☑ Send Mail

Configuring the SSL Certificate

This screen allows you to either create the certificate required for the Certificate Signing Request (CSR) or upload an existing certificate. A certificate is necessary when using a browser to access a secure (HTTPS) site. The HTTPS scheme requires that a digitally signed certificate is installed at the applicant's site.

- "To Generate a New CSR" on page 28
- "To Upload an Existing Certificate" on page 29

▼ To Generate a New CSR

1. **From the Configuration submenu, click the SSL Certificate tab.**

   The SSL Configuration screen appears.

2. **In the drop-down list, select CSR.**

3. **Click the Select button.**

4. **Fill in the open fields, and click the Generate button.**

▼ To Upload an Existing Certificate

1. **From the Configuration submenu, click the SSL Certificate tab.**

   The SSL Configuration screen appears.

2. **In the drop-down list, select Certificate.**

3. **Click the Select button.**

4. **Click Browse, and select the SSL Certificate.**

5. **Click Upload.**

Configuring ADS

▼ To Configure ADS

1. **From the Configuration submenu, click the ADS Configuration tab.**

   The ADS Configuration screen appears. The ADS Configuration screen allows you to locate and upload a certificate from Active Directory Service (ADS) for a Microsoft Windows environment. Using ADS can simplify administration tasks by allowing the monitoring of several machines in one node.

2. **Click Browse... to locate the ADS certificate.**

3. **Enter the Primary, Secondary DNS, and Root Domain addresses**

4. **Click Submit, or click Reset to clear your changes.**

Configuring SNMP

▼ To Configure SNMP

1. **From the Configuration submenu, click the SNMP tab.**

   The SNMP screen appears, and the SNMP Settings, SNMP Communities, and SNMP User Settings submenu tabs become available.

▼ To Configure SNMP Settings

1. **From the SNMP submenu click the SNMP Settings tab.**

   The SNMP Settings screen appears. On this screen you can designate the port, set requests, and select versions of SNMP protocols to be permitted.

   See Chapter 8 for a description of the meaning of those choices.

2. **Select the Set Request check box to set one or more SNMP variables.**

   This check box acts as a global override for the user and community read/write permissions. For example, if you disable Set Requests, a member of the private community accessing your Sun server module or stand-alone system via the SNMP interface cannot set sysContact despite having write permission.

3. **To override the delivered system default, select the check box beside the preferred version of SNMP protocols.**

4. **Click Submit, or to clear your entries, click Reset.**

▼ To Configure SNMP Communities

1. **From the SNMP tab, choose SNMP Communities.**

   The SNMP Communities screen appears. This screen allows you to add, modify, and delete SNMP Communities.

2. **To add, modify, or delete a community, click the radio button for the row that you would like to configure.**

3. **In the same row, click the appropriate Operation button.**

   The Add and Modify buttons take you to screens, where you have the option to name the community and configure the community permission. The two permission options are read-only (ro) or read/write (rw). The Delete button deletes the community *without* a confirmation prompt.

4. **Click Submit to save your changes.**

   You can also click Reset to cancel without saving.

▼ To Configure SNMP Users

1. **From the SNMP submenu, click SNMP User Settings.**

   The SNMP User Settings screen appears. This screen allows you to add a new user, and edit an existing user's settings.

2. **To add, edit, or delete a user, select the radio button at the head of the row in which you would like to work.**

3. **In the same row, click the appropriate Operation button.**

   - Clicking the Delete button deletes the user *without* a confirmation.
   - Clicking the Add and Edit buttons take you to the User Setting screen where you can enter the user name and password, and set the user permission. The two permission options are read-only (ro) or read/write (rw).

4. **Click Submit to save your changes.**

   You can also click Reset to cancel without saving.

Managing the System

This section contains the following system management procedures:

- "Managing User Accounts" on page 31
- "Managing the System Indicator and Fault LED" on page 35

Managing User Accounts

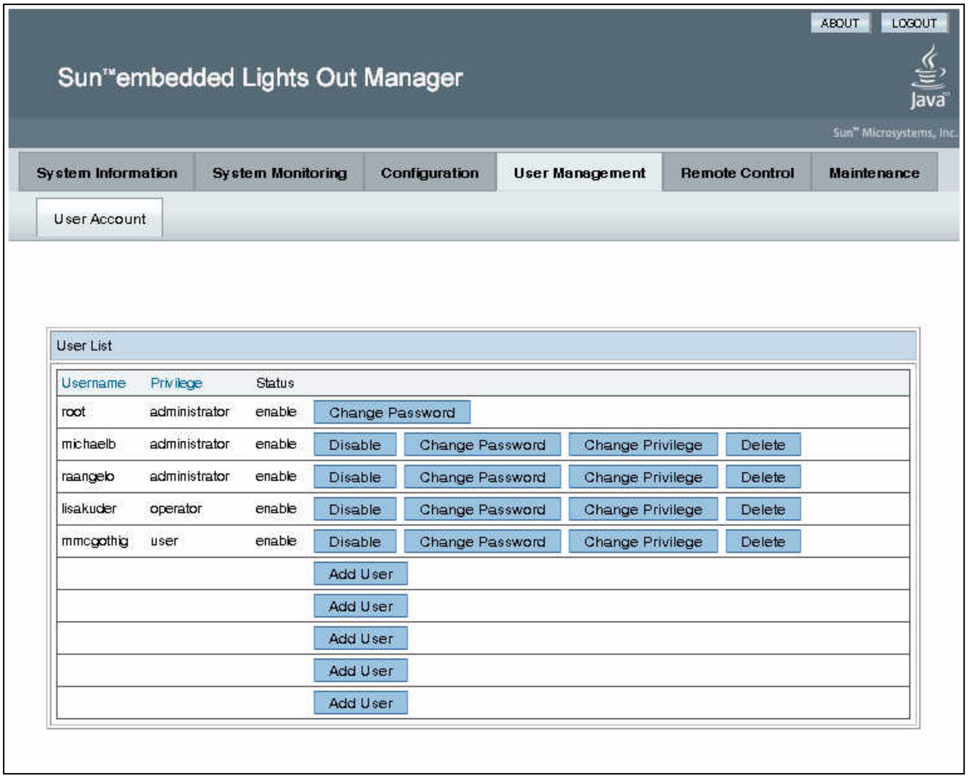
The User Management tab allows you to access the User Account screen to create new user accounts, and modify existing ones. You can manage who has access to the ELOM. You can also designate a user's level of access. This allows you to set up a hierarchy of users, and manage the security for your server.

▼ To Manage User Accounts

1. **From the main menu, click the User Management tab.**

   The User Account screen appears (see FIGURE 4-3). The User Account screen shows the User List, which allows you to add or delete a user, change a user password and privilege, and enable or disable a user's status.

FIGURE 4-3 The User Account Screen Showing the User List



User List

Username	Privilege	Status				
root	administrator	enable	Change Password			
michaelb	administrator	enable	Disable	Change Password	Change Privilege	Delete
raangelo	administrator	enable	Disable	Change Password	Change Privilege	Delete
lisakuder	operator	enable	Disable	Change Password	Change Privilege	Delete
mmcgothig	user	enable	Disable	Change Password	Change Privilege	Delete
			Add User			
			Add User			
			Add User			
			Add User			
			Add User			

The ELOM supports up to ten user accounts. One of the user accounts is root, which is the default account. It cannot be deleted or modified. Therefore, you can configure up to nine additional accounts.

Note – The only user field that you can change for the root account is the password.

Each user account consists of a user name, a password, and a privilege. The user name and password must be 8-16 characters in length.

The available privileges are:

- **Administrator** – Enables access to all ELOM software features, functions, and commands. If a new user is given administrator privileges, those privileges are also automatically granted for the command-line interface (CLI) and Intelligent Platform Management Interface (IPMI) to the service processor's Sun Blade X6250 server module software.
- **Operator** – Enables limited access to SP software features, functions, and commands.
- **User** and **Callback** – Enables limited access to the system on a read-only basis.

Note – If the SP password has been changed and then lost, a BIOS option exists to reset the password back to the default `changeme`. See "Resetting the BMC/SP" on page 36.

▼ To Add a User

Note – Only accounts with Administrator privileges are allowed to add, modify, or delete user accounts.

---

1. **From the User Management main menu, click the User Account tab.**

   The User List screen appears.

2. **In User List screen, click any available Add User button.**

   The Manage User Account screen appears.

Note –

---

3. **Enter a user name and password in their respective fields.**

   The user name and password must be 8-16 characters in length. Both are case-sensitive. You can use alphabetical characters, numerals, hyphens, and underscores. Do not include spaces in user names and passwords.

4. **Enter the password again in the Confirm Password field.**
5. **Select either Administrator, Operator, User, or Callback for the user role.**
6. **Click Submit to create the user.**

▼ To Delete a User Account

1. **In the User List, locate the user name of the account you want to delete.**
2. **Click the Delete button for the account.**

   The system will *not* prompt for a confirmation.

▼ To Change a User Account Password or Privilege

1. **From the User Management main menu, click the User Account tab.**

   The User List screen appears.
2. **In the User List screen, click the Change Password or Change Privilege button for the appropriate user account.**

   The Manage User Account screen appears.
3. **In the Manage User Account screen, make the necessary changes, and click Submit.**

▼ To Enable or Disable a User Account

1. **From the User Management main menu, click the User Account tab.**

   The User List screen appears.
2. **To disable or enable a user account, click the Disable or Enable button for that account.**

Managing and Maintaining the Server

This section contains the following server management and maintenance procedures:

- "Controlling Server Power" on page 36
- "Resetting the BMC/SP" on page 36
- "Updating the Firmware" on page 38
- "Updating the CPLD (Common Programmable Logic Device)" on page 41

- “Recovering from a Corrupt Service Processor” on page 42
- “Setting Session Timeout” on page 44
- “Setting the Time” on page 44

Managing the System Indicator and Fault LED

The System Indicator (Locator) LED is located on the front of the server. You can activate the indicator LED in the ELOM. By activating the indicator LED for a particular server, you can identify that server from the many other servers installed in a chassis. Similarly, the Fault LED allows you to quickly identify a server that is in a fault state. You can see the state of the Fault LED, and control the state of the System Indicator LED from the ELOM System Monitoring screens.

▼ To Control the State of the System Indicator LED

1. **From the main menu, Click the System Monitoring tab.**

   The System Monitoring submenu tabs appear.

2. **Click the System Indicator submenu tab.**

   The System Indicator LED screen appears.

3. **Select the appropriate radio button to either turn the LED on or turn it off.**

4. **Click Submit to change the state of the LED, or click Reset to cancel.**

▼ To View the State of the Fault LED

1. **In the main menu, Click the System Monitoring tab.**

   The System Monitoring submenu tabs appear.

2. **Click the Fault LED submenu tab.**

   The Fault LED Control screen appears. The current status of the LED is displayed as either On or Off.

Controlling Server Power

You can control power to the server you are logged-in to by using the Remote Power Control submenu screen. The Remote Power Control screen allows you to power the server off, reset the server, boot to the BIOS setup, or boot off Pc-Check.

▼ To Control Server Power

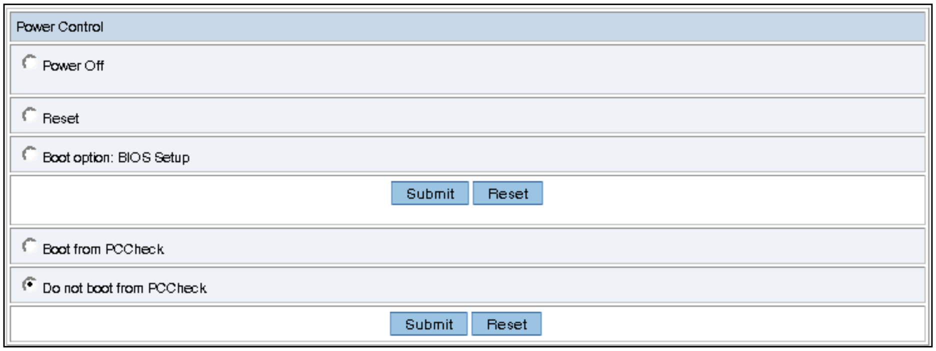
1. **From the main menu, click the Remote Control tab.**

   The Redirection, Remote Power Control, and Hotkey Setup submenu tabs appear.

2. **Click the Remote Power Control submenu tab.**

   The Power Control screen appears (see FIGURE 4-4).

FIGURE 4-4 The Power Control Screen



Power Control

○ Power Off

○ Reset

○ Boot option: BIOS Setup

○ Boot from PCCheck

● Do not boot from PCCheck

3. **Click the radio button for the power control option that you need.**

4. **Click Submit to initiate the power control option.**

Resetting the BMC/SP

The baseboard management controller (BMC)/service processor (SP) holds the original default settings. In the event of system lock-up or loss of the root password, you can reset the BMC to return to the original default settings. This procedure requires you to log in to the ELOM web GUI, access the Maintenance submenu screens and initiate the reset.

Note – To reset the BMC/SP password without reverting the SP to the default settings, see the next procedure, "Resetting the BMC/SP Password" on page 37.

▼ To Reset the BMC/SP

1. **Log in to the ELOM web GUI using an account with administrator privileges.**

   The ELOM web GUI main menu appears.

2. **From the main menu, click the Maintenance tab.**

   The Maintenance submenu tabs appear.

3. **Click the Reset BMC tab.**

   The Reset BMC screen appears.

Note – Resetting the BMC is a hard reset. If you are logged in, when the BMC (SP) is reset, you will be logged off. You will need to wait a couple of minutes before you can log in again.

4. **Click the Reset BMC button.**

   The following message appears:

   "Please wait for BMC reset then reconnect."

Resetting the BMC/SP Password

This procedure enables you to use the server's BIOS Setup Utility to reset the SP (BMC) password. Unlike the previous procedure, this procedure allows you to reset the password *without* reverting the SP to its default settings. This procedure requires that you reboot the server, access the BIOS Setup Utility screens, navigate to the Server screen, and imitate the reset.

Note – To reset the SP password and revert the SP to the default settings, see the previous procedure, "Resetting the BMC/SP" on page 36.

▼ To Reset the BMC/SP Password

1. **Use the multi-port cable and the UCP connector on the front of the server module to set up the server to view POST messages.**

   For more information, see the *Sun Blade X6250 Server Module Installation Guide*.

2. **Reboot the server and watch the screen.**

   At the splash screen, you are prompted to press F2 to enter the BIOS Setup Utility.

3. **Press F2.**

   The BIOS Setup Utility main screen appears.

4. **Use the left or right arrow keys to navigate to the Server screen.**

   The Server screen appears.

5. **Use the down arrow key to navigate to the Reset BMC Password field.**

6. **To reset the BMC password, press Enter.**

   A prompt appears to confirm the reset.

7. **To confirm the reset, press Enter.**

8. **Press F10 to save and exit.**

   The server reboots and the BMC/SP password is reset to changeme.

Updating the Firmware

There are multiple ways to update the SP firmware:

1. Use `tftpupdate` through the CLI. See "To Update the Firmware" on page 68.
2. Use the web GUI firmware update. See the next section, To Update the Firmware Using the Web-based Interface.

▼ To Update the Firmware Using the Web-based Interface

1. **Power off the server.**

   To power off the server using the web GUI, see "Controlling Server Power" on page 36.

2. **At the Sun Download Center, navigate to the Sun Blade X6250 server module page, and download the following file:**

   `x6250v*.rom`

   where * is the file version number.

3. **Login in to the web GUI using an account with administrator privileges.**

   The ELOM main screen appears.

4. **From the main menu, click the Remote Control tab.**

   The Remote Control submenu tabs appear.

5. **Click the Remote Power Control tab.**

   The Remote Power Control screen appears.

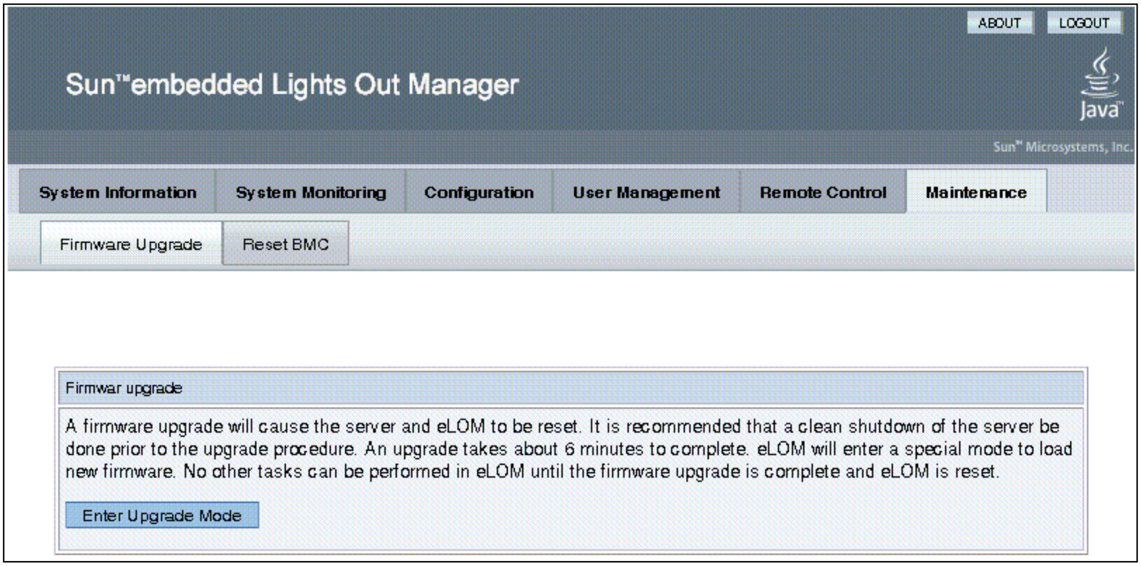
6. **Select Power Off radio button, and click the Submit button.**

   This action powers off the server.

7. **From the main menu, click the Maintenance tab.**

   The Maintenance submenu tabs appear (see FIGURE 4-5).

FIGURE 4-5 The Firmware Upgrade Screen



A firmware upgrade will cause the server and eLOM to be reset. It is recommended that a clean shutdown of the server be done prior to the upgrade procedure. An upgrade takes about 6 minutes to complete. eLOM will enter a special mode to load new firmware. No other tasks can be performed in eLOM until the firmware upgrade is complete and eLOM is reset.

8. **Click the Firmware Upgrade tab.**

   The Firmware Upgrade screen appears.

9. **Click the Enter Firmware Upgrade Mode.**

10. **Locate the firmware upgrade file.**

    a. **Click Browse.**

    b. **Browse for the** `x6250v*.rom` **file.**

    c. **Select the file, and then click Open.**

11. **Click the Update Firmware button to start the firmware upgrade.**

    The firmware upgrade process updates the BIOS and the ELOM. After the upgrade is complete, the ELOM reboots and the web session is restarted.

12. **Power on the server, open a browser, and log in to the web GUI.**

Note – The BIOS version information is updated once the host is powered on.

---

13. **From the main menu, click the Remote Control tab.**

14. **In the Remote Control submenu screen, click Launch Redirection.**

    The RKVM screen comes up. The RKVM screen *might* display the message:

```
Error (0005) : CMOS Checksum Bad
Press F2 to run SETUP
Press F1 to load default values and continue.
```

- If the RKVM screen *does not* display a checksum message, then you are done, and the system boots.
- If the RKVM screen *does* display a checksum message, proceed to the next step, Step 15.

Note – The checksum error is not a problem. The message indicates that the checksum for the new BIOS is different from the original.

---

15. **If the RKVM screen displays the checksum error message shown in the previous step, either load optimal defaults or change BIOS settings. Do one of the following:**

- Load optimal defaults:

    a. **Press F1 to load optimal default values and continue.**

    The system resets the BIOS settings back to defaults and boots. Go to Step 16.

    -or-

- Change BIOS settings:

a. **Press F2 to enter the BIOS Setup.**

   The BIOS main menu appears.

b. **Press F9 to load optimal defaults.**

c. **Change the BIOS settings.**

d. **Save your settings, and exit BIOS Setup.**

16. **The server boots.**

Updating the CPLD (Common Programmable Logic Device)

The following procedure is rarely used, and should not be done unless instructed by Sun Service personnel.

▼ To Update the CPLD

1. **Download the Tools and Driver CD ISO image at:**

   `http://www.sun.com/servers/blades/downloads.jsp`

2. **Burn a CD, or mount the downloaded ISO image.**

3. **Locate the following combined firmware image file:**

   `firmware/bmc/CPLD_V*.jbc`

   where * is the file version number.

4. **Save the** `CPLD_V*.jbc` **file to a location on your hard drive.**

5. **Login to the ELOM web GUI.**

6. **From the main menu, click the Remote Control tab.**

   The Remote Control submenu tabs appear.

7. **Click Remote Power Control submenu tab.**

   The Remote Power Control submenu screen appears.

8. **Select the Power Off radio button, and click Submit.**

   The OS must be shut down.

9. **From the main menu, click the Maintenance tab.**

   The Maintenance submenu screen appears.

10. **Click Enter Upgrade Mode.**
11. **Click Browse and select the** `CPLD_V*.jbc` **file.**

    where * is a variable that identifies the file version number.
12. **Select Upgrade to upgrade the CPLD.**
13. **Wait until the upgrade is finished.**
14. **Power cycle or reset the server to enable the new CPLD to take effect.**

Recovering from a Corrupt Service Processor

Should the service processor (BMC) software become corrupted, you can reinstall the default image from the CD. You will need to remove the server from the chassis, and short the connections on jumper block J19 on the motherboard.

To perform this procedure, you have must have a bootable USB flash device to load files and boot the server module, a jumper to short the pins on jumper block J19, and a KVM attached to the server module to monitor the recovery process and respond to system prompts.

Note – To properly perform this procedure and the procedures referenced in the following steps, see the *Sun Blade X6250 Service Manual*.

Caution – Irreparable damage to server motherboard and system components can occur from electrostatic discharge. These components are extremely sensitive to static electricity. Before touching or handling printed circuit boards and components, attach an ESD wrist strap to bare metal on the chassis or the grounding post that is built into the rear of the chassis.

▼ To Recover from a Corrupt Service Processor

1. **Copy all BMC files from the Tools and Drivers CD to a *bootable* USB flash device.**

   The BMC files are located in the `/firmware/bmc` directory, on the Tools and Drivers CD. They consist of:

   - SOCFLASH.EXE
   - DOS4GW
   - BMC Binary *(SP Binary file)*

2. **Power off the server gracefully.**

Note – Do not attempt to flash the system while it is still powered on. An unrecoverable error may occur.

---

3. **Remove the server module from the chassis.**

4. **Place the server module on an anti-static mat, and remove the top cover.**

5. **Put on the ESD wrist strap, and attach the grounding clip to the chassis' bare metal or the chassis grounding post.**

6. **Locate jumper block J19, and use a jumper to short the pins.**

   See the *Sun Blade X6250 Service Manual* for the location of jumper block J19.

7. **With the pins on jumper block J19 shorted, remove the wrist strap grounding cord from the chassis, and replace and secure the top cover.**

8. **Insert the server module into the chassis.**

9. **Insert the bootable flash drive into the USB port.**

10. **Power on the system.**

    A message will appear on the video console stating that the BMC was not found. The system will take up to three minutes to boot.

11. **Press F8 to get a list of boot devices.**

12. **Set the USB flash device as the primary boot device, and save and exit.**

    The server module boots from the USB flash device.

13. **When the server finishes booting, run the following command:**

    `socflash.exe` *SP binary backup file*

    For example:

    ```
    socflash.exe s40v092.bin backup.bin
    ```

14. **After a successful flash, remove the server module from that chassis, and remove the jumper from jumper block j19.**

15. **Insert the server module into the chassis, leaving the system powered off for at least 30 seconds.**

16. **Power on the system; watch the display, and when prompted, press F2 to enter the BIOS Setup Utility.**

17. **Verify the status of the BMC and the BMC version in the BIOS Setup Utility under the** `Advanced/IPMI` **screen.**

Setting Session Timeout

The Session Time-Out is an inactivity timer. If an open session enters a state of inactivity that exceeds the preset timer, the system will close (log out) the session. This function prevents unauthorized access to the system by providing an automated log-out function. To use the session timeout function, you must first enable it.

▼ To Set the Session Timeout

1. **From the main menu, click the System Information tab.**

   The Versions, Session Time-Out, and Components submenu tabs appear.

2. **Select the Session Time-Out tab.**

   The Session Time-Out screen appears.

3. **Click the Enable Timeout radio button.**

4. **Select a session time from the Session Time drop-down list.**

   The options are 15 minutes (default), 30 minutes, 1-hour, and 2 hours.

5. **Click the Submit button to set the session timeout.**

Setting the Time

▼ To Set Time

1. **From the Configuration submenu, click the Set Time tab.**

   The Set Time screen appears. Use the radio buttons to manually input the date and time.

CHAPTER 5

Using the Remote Console Application

This chapter describes how to use the remote console application. It includes the following sections:

Accessing the Remote Console From the Web GUI

The remote console application, which is started using the web GUI, enables you to control your server's operating system remotely using the screen, mouse and keyboard, and to redirect local CD and diskette drives as if they were connected directly to the server.

Installation Requirements

A compatible browser and a minimum of JRE™ 1.6.0 are required to operate the remote console application. See TABLE 5-1.

Note – You do not need to install any OS-specific drivers or helper applications on client systems to run the remote console application.

TABLE 5-1 Client Installation Requirements

Client OS	Java Runtime Environment Including Java Web Start	Browsers
Microsoft Windows XP Pro	JRE 1.6 (Java 6.0 or later)	Internet Explorer 6.0 and later Mozilla 1.7.5 or later Mozilla Firefox 1.0
Red Hat Linux 4.0 or later Desktop and Workstation Editions	JRE 1.6 (Java 6.0 or later)	Mozilla 1.7.5 or later Mozilla Firefox 1.0
Solaris 9	JRE 1.6 (Java 6.0 or later)	Mozilla 1.7.5
Solaris 10	JRE 1.6 (Java 6.0 or later)	Mozilla 1.7.5
SUSE Linux 9.2	JRE 1.6 (Java 6.0 or later)	Mozilla 1.7.5

Note – You can download the JRE 1.6 at `http://java.com`.

CD and Diskette Redirection Operational Model

When you redirect the local client CD drive or diskette drive to a remote host server, the following rules apply:

- In all cases, the CD drive and diskette drive appear to be plugged in to the host.
- If you do not redirect them, the host will act as if there is no medium unless there is a CD in the host CD drive. If there is a CD in the host CD drive, the host accesses it normally.

The information in TABLE 5-2 describes different case scenarios in which the remote console application and CD drive and diskette drive redirection operate.

TABLE 5-2 Remote Console Operation With CD Drive and Diskette Drive

Case	Status	CD As Seen by Host	Diskette As Seen by Host
1	Remote console application not started or remote console started but CD/diskette redirection not started.	CD device present. No medium indication is sent to the host from the ELOM whenever the hosts asks.	Diskette device present. No medium indication is sent to the host from the ELOM whenever the host asks.
2	Remote console application started with no medium present in the drive.	CD device present. Whenever the host asks, which may be automatic or when you access the device on the host, the remote client sends a status message. In this case since there is no medium, the status is no medium.	Diskette device present. Whenever the host asks (for example, you double-click a drive), the remote client sends a status message. In this case since there is no medium, the status is no medium.
3	Remote console application started with no medium, then medium is inserted.	CD device present. Whenever the hosts asks (automatic or manual), the remote client sends a status message as medium present and also indicates the medium change.	Diskette device present. Whenever the host asks (manual), the remote client sends a status message as medium present and also indicates the medium change.
4	Remote console application started with medium inserted.	Same as 3.	Same as 3.
5	Remote console application started with medium present, then medium is removed.	Next command from the host will get a status message indicating medium not present.	Next command from the host will get a status message indicating medium not present.
6	Remote console application started with image redirection.	Same as 3.	Same as 3.
7	Remote console application started with image, but redirection is stopped (which is the only way to stop ISO redirection).	Driver knows CD redirection stopped so it sends a medium absent status on the next host query.	Driver knows CD redirection stopped so it sends a medium absent status on the next diskette query.
8	Network failure.	The software has a keepalive mechanism. The software will detect keepalive failure since there is no communication and will close the socket, assuming the client is unresponsive. Driver will send a no medium status to the host.	The software has a keepalive mechanism. The software will detect unresponsive client and close the socket, as well as indicate to the driver that the remote connection went away. Driver will send a no medium status to the host.
9	Client crashes.	Same as 8.	Same as 8.

Starting the Remote Console Application

Use this procedure to start the remote console application from the web GUI. You may be presented with a series of questions. In each case, select Run.

Note – Each new ELOM system is delivered with DHCP set as the default. If an IP address is not found within 5 seconds, the system will default to the IP address `192.168.1.2` to allow instant web access.

▼ To Start the Remote Console Application

1. **Open your browser.**
2. **In the address bar, enter the IP address of the SP that you obtained in:** "To Set Up the Service Processor with the WebGUI" on page 23**.**

   The login screen appears.
3. **Type user name and password for an account with administrator privileges.**
4. **Click Login.**

   The ELOM main menu appears.
5. **Click the Remote Control tab.**
6. **Select Redirection.**

   The screen displays a Launch Redirection button.
7. **Click Launch Redirection.**

   A screen identifies your current host name, IP address, and user name. The Launch button opens the remote console.
8. **Click Launch.**

Note – For systems using Firefox and Mozilla browsers, the required version of JRE must be at least version 1.6 or later.

The browser downloads the embedded remote control application automatically, and the Remote Console screen appears.

Note – If the remote console does not display, it might be blocked by browser security controls (pop-up blocker). Reduce security configuration to allow the remote console to display.

Redirecting Keyboard, Video, Mouse, or Storage Devices

The remote console application supports the redirection of the following types of devices:

- Video quality display – the server's video output is automatically displayed on the local console screen.
- Hot key – enable a single key to mimic a series of keystrokes.
- Keyboard and mouse devices – Standard keyboards, mouse, and other pointing devices.
  - Keyboard redirection is enabled by default.
  - Mouse redirection must be enabled manually.
- Storage devices – CD/DVD drives, Flash, DVD-ROM or diskette disk drives, hard drives, or NFS.

▼ To Redirect Keyboard and Mouse Devices

Use the following procedure to redirect your local workstation or laptop keyboard and mouse to a remote Sun Blade X6250 server module.

1. **Start the remote console application as described in** "Starting the Remote Console Application" on page 48**.**

2. **From the system management software opening screen select the Remote Control tab.**

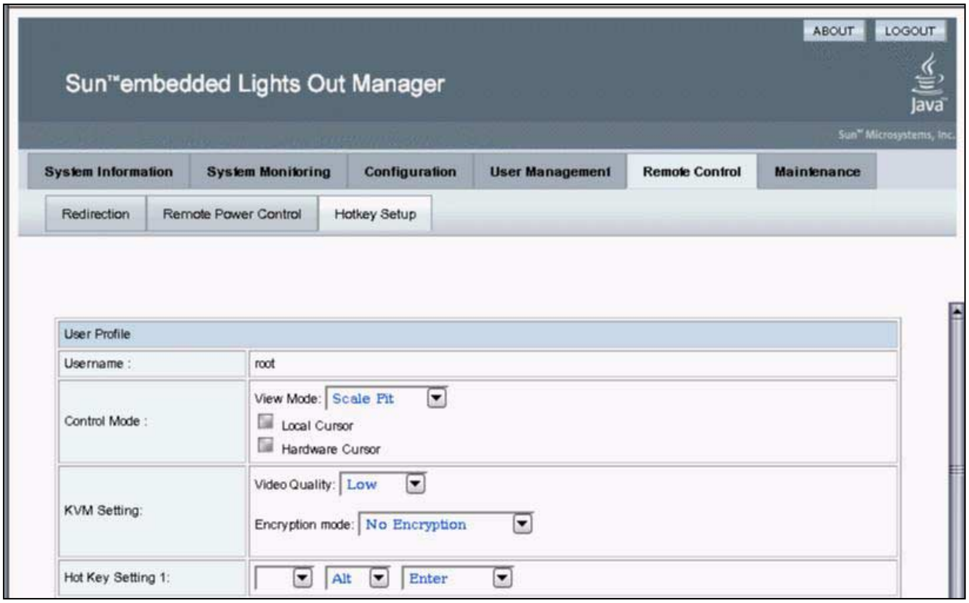
3. **Select the Hotkey Setup tab.**

   The Control Mode section of the Hotkey Setup screen enables mouse redirection.

4. **Select Hardware Cursor to enable a variety of cursor movements.**

Note – For the mouse to work correctly, you might have to change the mouse mode. Click the double mouse cursor on the navigation bar to toggle between local and remote mouse cursor movement. Keyboard redirection is selected by default.

FIGURE 5-1 Keyboard, Video, and Mouse Selections



User Profile	
Username :	root
Control Mode :	View Mode: Scale Fit □ Local Cursor □ Hardware Cursor
KVM Setting:	Video Quality: Low Encryption mode: No Encryption
Hot Key Setting 1:	Alt Enter

You can click Submit to enable your options after each choice to observe the consequences, or continue directly to Step 5.

5. **When you have completed your selections, click Submit to enable your options.**

▼ To Redirect Storage Devices

Use the following procedure to enable a storage device attached to your local workstation or laptop to serve as a storage device for a server module. You can use this option to install software from a local CD/DVD drive to multiple remote servers.

You can also redirect a CD image file or a diskette image file stored on your hard drive.

1. **Start the remote console application as described in "Starting the Remote Console Application" on page 48.**

   The Remote Console screen is displayed.

2. **Select Storage from the drop-down list and click Mount Device.**

   This enables the corresponding local storage device to connect to the remote server as though it were a storage device attached directly to that remote server.

3. **Select a source device from the drop-down list.**

   - To store a selection to a real CD-ROM device, select from the Drive Name drop-down list.
   - To store a CD image file or a diskette image file to your hard drive, select ISO file from the Source Device drop-down list.

Note – You cannot select two CD-ROM devices or two diskette devices. For example, you cannot select CD-ROM and CD-ROM image. Use the browser to navigate to the corresponding file, then click Submit.

After successfully mounting a storage device a green check mark is displayed in the lower left corner of the Remote Console window.

Note – Use the web GUI to disable the session time out, or to set the session timeout to a long enough period of time to allow you to work without the system automatically logging you out.

Installing an OS on a Remote Server

This method includes using a CD or DVD drive or image of the operating system on a remote networked system to install the operating system, for example, onto the Sun Blade X6250 server module.

Requirements for Remote KMVS Over IP installation include:

- Remote system connected to the network
- CD/DVD drive connected to the remote system
- Media for installing the operating system of your choice
- SP of the server set up as instructed in the *Sun Blade X6250 Server Module Installation Guide*.

▼ To Install an OS on a Remote Server Using a Virtual CD-ROM

Note – Disable the timeout function when installing remotely from the virtual CD-ROM.

---

1. **On your laptop or local terminal, open a browser, and enter the IP address of the Sun Blade X6250 server module service processor for the target system.**

   This is the Sun Blade X6250 server module on which you want to install the operating system.

2. **Enter the user name and password in the login screen.**
3. **In the main ELOM screen, click the Remote Control tab, then click Launch Redirect to open a remote console screen.**
4. **Insert the operating system CD/DVD to be installed on the Sun Blade X6250 server module into your laptop or local CD/DVD drive.**
5. **In the remote console screen, choose Storage –>Mount devices.**

   The Device Configuration screens appears.

6. **Under Storage 1, in the drop-down list, select the local CD/DVD that you will be using for the installation.**
7. **Click Submit.**
8. **Reboot the server.**

Other Remote Options

Command-line options that are available to address many of these tasks include IPMI tools (Chapter 7), CLI (Chapter 6), and SSH (Secure Shell).

CHAPTER 6

Using the Command-Line Interface

This chapter describes how to use the Embedded Lights Out Manager (ELOM) command-line interface (CLI). The sections include:

Logging In to the CLI

You can access the command-line interface through the serial port or over the Ethernet.

- Serial port – The serial port provides access to the CLI and to the system console. IPMI terminal mode and PPP mode are not available on the serial port.
- SSH – You can connect to the CLI using an Ethernet connection. Secure shell (SSH) connections are enabled by default.

The Sun Blade X6250 server module ELOM supports a maximum of 10 active sessions, including serial, SSH, and web interface sessions.

Note – Telnet connections to the ELOM are not supported.

▼ To Log In Using SSH

This section describes how to log in to the service processor using Secure Shell.

1. **If necessary, start your SSH client**
2. **Access the system command-line.**
3. **Log in to the ELOM using a user account that has administrator privilege, by entering the following command:**

   ```
   $ ssh administrator_account@ipaddress
   ```

   administrator_account An account with administrator privileges.
   ipaddress The IP address of the service processor.

   A password prompt appears.

4. **Enter the password when prompted.**

   For example:

   ```
   $ ssh root@192.168.25.25
   root@192.168.25.25's password:changeme
   Sun (TM) Embedded Lights Out Manager
   Version 1.0
   Copyright 2006 Sun Microsystems, Inc. All rights reserved.
   Warning: password is set to factory default.
   ->
   ```

▼ To Log In From the Serial Port

This section describes how to log-in to the service processor from the serial port using a terminal device.

1. **Configure your terminal device or the terminal emulation software running on a laptop or PC to the following settings:**
   - 8N1: eight data bits, no parity, one stop bit
   - 9600 baud
   - Disabled software flow control (CTS/RTS)
2. **Connect a serial cable from the server RJ-45 Serial Mgt port to a terminal device.**

   An RJ-45 to DB9 cable is included with your server.

3. **Press the Enter key on the terminal device to establish a connection between that terminal device and the SP.**

   You should see the following prompt:

   ```
   SP ->SUNSP0016364A9934 login:
   ```

4. **Log in to the SP and enter the user name and password.**

   The default user name is **`root`**, and the default password is **`changeme`**.

Note – Once you have logged in to the SP as root, change the default password for increased security.

Note – If you have changed the serial redirection output in the system BIOS from BMC (that is, from the SP) to system, the system output will be displayed on the serial connection. To view the SP output on the serial connection, change the system BIOS back to the default BMC.

Command Syntax

The CLI architecture is based on a hierarchical namespace, which is a predefined tree that contains every managed object in the system. This namespace defines the targets for each command verb. The top of the hierarchical structure is designated by /. Namespaces directly below are /SP, /SYS, and /CH.

The /SP namespace allows you to manage, maintain, and configure the server. Children of this namespace include `/users` and `/network`, and, `/AgentInfo`.

The /SYS namespace allows you to view your server's system information.

The /CH namespace allow you to view chassis information.

The CLI provides four privilege levels: administrator, user. operator, callback. Only the administrator privilege has full read and write access to all ELOM functionality.

Note – The default user, root, has administrator privileges. For information about how to create a user account with user privileges, see "To Add a User Account" on page 62.

CLI commands are case-sensitive.

Syntax

The syntax of a command is *verb options target properties*.

Command Verbs

TABLE 6-1 describes the CLI command verbs.

TABLE 6-1 CLI Command Verbs

Command	**Description**
`cd`	Navigates the object namespace.
`create`	Sets up an object in the namespace.
`delete`	Removes an object from the namespace.
`exit`	Terminates a session to the CLI.
`help`	Displays Help information about commands and targets.
`load`	Used to transfer a file from a server to update a target.
`reset`	Resets the target's state.
`set`	Sets target properties to the specified value.
`show`	Displays information about targets and properties.
`start`	Starts the target.
`stop`	Stops the target.
`version`	Displays the version of ELOM firmware that is running.

Options

The CLI supports the following options. However, not all options are supported for all commands. The only option that works with all commands is `-help`. Refer to a specific command section in this document or use the `-help` option to list the options that are valid for a particular command.

TABLE 6-2 CLI Options

Option Long Form	Short Form	Description
`-default`		Causes the verb to perform only its default functions.
`-destination`		Specifies the destination for data.
`-display`	`-d`	Shows the data you want to display.
`-examine`	`-x`	Examines the command but does not execute it.
`-force`	`-f`	Causes an immediate action instead of an orderly shutdown.
`-help`	`-h`	Displays Help information.
`-keep`	`-k`	Establishes a holding time for command job ID and status.
`-level`	`-l`	Executes the command for the current target and all targets contained through the level specified.
`-output`	`-o`	Specifies the content and form of command output.
`-resetstate`		Indicates to what target-specific state to reset the target.
`-script`		Skips warnings or prompts normally associated with the command.
`-source`		Indicates the location of a source image.

Targets

Every object in your namespace is a target. Not all targets are supported for all commands. Each command section lists the valid targets for that command.

Properties

Properties are the configurable attributes specific to each object. An object can have one or more properties. Each command section lists the valid properties for each target.

Managing the Host

You can use the ELOM to change the host's state and to access the host console.

Managing the Host State

▼ To Manage the Host State

- **To power on the host, enter the following command:**

```
–> set /SYS/CtrlInfo PowerCtrl=on
```

- **To power off the host gracefully, enter the following command:**

```
–> set /SYS/CtrlInfo PowerCtrl=gracefuloff
```

- **To power off the host, enter the following command:**

```
–> set /SYS/CtrlInfo PowerCtrl=off
```

- **To reset the host, enter the following command:**

```
–> set /SYS/CtrlInfo PowerCtrl=reset
```

- **To reboot and enter the BIOS automatically, enter the following command:**

```
–> set /SYS/CtrlInfo BootCtrl=BIOSSetup
```

- **To reboot and enter PXE automatically, enter the following command:**

```
–> set /SYS/CtrlInfo BootCtrl=PXE
```

- **To reboot and enter Pc-Check diagnostic automatically, enter the following commands:**

```
–> set /SYS/CtrlInfo PowerCtrl=PCCheck_enable
–> set BootCtrl=PCCheck_enable
```

- **To disable the option to boot to Pc-Check, and set the option to boot normally, enter the following commands:**

```
–> set BootCtrl=regular
–> set /SYS/CtrlInfo BootCtrl=PCCheck_disable
```

Managing the Host Console

You can manage the host console by using the `start` and `stop` commands.

▼ To Manage the Host Console

To start a session to the server console, enter this command:

```
-> start /SP/AgentInfo/Console
```

Note – After running the `start` command, no output will be displayed until the server is rebooted.

To revert to CLI once the console has been started, press **`Esc-Shift-9`** (**`Esc-(`**).

Note – Key combinations in this manual are based on the U.S. keyboard, which might differ from other keyboards. For a U.S. keyboard map, see Appendix B.

Enter this command to terminate a server console session started by another user:

```
-> stop /SP/AgentInfo/Console
```

Viewing Host Sensors

Host systems are equipped with sensors that read the state of critical components. For example, the sensors read temperatures, voltages, and fan speeds.

▼ To View Host Sensors

The `show` command can be used to show the state of sensors. Use the command:

```
-> show /SYS/CPU/sensor
```

sensor The particular sensor.

For example, the following command shows the state of sensor /CPU/CPU0:

```
-> show /SYS/CPU/CPU0
```

For more information about sensors, including how to view them using a browser, see "Monitoring the System" on page 19.

For details on individual sensors, see your platform supplement.

Managing ELOM Network Settings

You can display or configure the ELOM network settings from the CLI.

▼ To Display network Settings

- **Enter the following command:**

```
–> show /SP/network
```

The above command displays the seven network properties, MACaddress, IPAddress, Netmask, Gateway, DNS, IPSource, and Hostname.

To display individual network settings, enter:
–> **show /SP/network** *property*

property One of the seven network properties.

▼ To Configure Network Settings

- **Use the** `set` **command to change a property's value.**

Tip – Ensure that the same IP address is always assigned to an ELOM by either assigning a static IP address to your ELOM after initial setup, or configuring your DHCP server to always assign the same IP address to an ELOM. This enables the ELOM to be easily located on the network.

Syntax

set /SP/network *property*=*value*

Targets, Properties, and Values

These targets, properties, and values are valid for ELOM network settings.

TABLE 6-3

Target	Property	Value
`/SP/network`	IPAddress	*ipaddress* | *none*
	Netmask	*xxx.xxx.xxx.xxx*
	Gateway	*IP address*
	DNS	*x.x.x.x*
	IPSource	*dhcp* | *static*

Examples

Note – Changing the IP address will disconnect your active session if you are connected to the ELOM via a network.

To change the IP address for the ELOM, enter:

–> **`set /SP/network IPAddress=`***xxx.xxx.xxx.xxx*

To set the Gateway address for the ELOM, enter:

–> **`set /SP/network Gateway=`***xxx.xxx.xxx.xxx*

To change the network settings from static to DHCP settings, enter:

–> **`set /SP/network IPSource=dhcp`**

Managing User Accounts

This section describes how to add, modify, and delete user accounts using the CLI.

The ELOM supports up to 10 user accounts. One of those, root, is set by default and cannot be removed. Therefore, you can configure up to 9 additional accounts.

Each user account consists of a user name, a password, and a permission.

The permissions are:

- **Administrator** – Enables access to all ELOM software features, functions, and commands. If a new user is given administrator privileges, those privileges are also automatically granted for the command-line interface (CLI) and Intelligent Platform Management Interface (IPMI) to the service processor's Sun Blade X6250 server module software.
- **Operator** – Enables limited access to SP software features, functions, and commands.
- **User** and **Callback** – Enables limited access to the system on a read-only basis.

The syntax is:

```
-> set permssion=[administrator|operator|user|callback]
```

▼ To Add a User Account

- **Enter the following commands:**

```
–> cd /SP/users
–> create username
```

username The name (8-16 characters in length) that the new user will use to log in to the ELOM. The system will then prompt you for a password (8-16 characters in length).

▼ To Delete a User Account

- **Enter the following command:**

```
–> delete /SP/users/username
```

▼ To Display User Accounts

- **Enter the following command:**

```
-> show /SP/users
```

▼ To Configure User Accounts

- **Use the `set` command to change passwords and permissions for configured user accounts.**

Note – You must have administrator privileges to change user properties.

Syntax

set target *[propertyname=value]*

Targets, Properties, and Values

These targets, properties, and values are valid for local user accounts.

TABLE 6-4

Target	Property	Value	Default
`/SP/users/username`	permission password	administrator | operator | user | callback *string* 8-16 characters in length	operator

Examples

When changing the permissions for user1234 from administrator to operator enter:

```
-> set /SP/users/user1234 permssion=operator
```

To change password for user1234, enter:

```
-> set /SP/users/user1234 password=new_password
```

Managing Alerts

The system is equipped with a number of sensors that measure voltages, temperatures, and other things. It polls the sensors and posts an event in the system event log (SEL) when they cross a threshold. Some of these readings are also used to perform actions such as adjusting fan speeds, illuminating LEDs, and powering off the chassis.

The alert management view allows you to configure the system to send alerts to IP addresses.

An alert is an IPMI platform event filter (PEF) generated when a sensor crosses the specified threshold. For example, if you configure an alert for critical thresholds, the SP sends an IPMI trap to the specified destination when any sensor crosses the upper or lower critical threshold (CT).

All alerts are IPMI PEF traps, as defined in the Intelligent Platform Management Interface (IPMI) v2.0.

Special informational criteria are reserved for system events that are not related to sensors.

▼ To Display Alerts

- **Enter the following command:**

  ```
  show /SP/AgentInfo/PEF
  ```

▼ To Configure Alerts

- **Use the** `set` **command to change properties and values for alerts from the CLI.**

Syntax

`set target` *[propertyname=value]*

Targets, Properties, and Values

These targets, properties, and values are valid for IPMI PEF alerts.

TABLE 6-5

Target	Property	Value	Default
`/SP/AgentInfo/PEF/`	PEFGlobalCtrl	disable | enable	disable
	PEFActionGlobalCtrlPowerOff	disable | enable	enable
	PEFActionGlobalCtrlPowerCycle	disable | enable	enable
	PEFActionGlobalCtrlPowerReset	disable | enable	enable
	PEFActionGlobalCtrlAlert	disable | enable	enable
	PEFActionGlobalCtrlMail	disable | enable	disable
	PEFActionGlobalCtrlInterrupt	disable | enable	disable

The parameters are:

- `rule` – The number of the alert rule. A number from 1 to 4.
- `ipaddress` – The IP address to which the alert will be sent.
- `level` – The severity level of the alert (see TABLE 6-6).

TABLE 6-6 Alert Levels

Alert Levels	Name in Sensor Readings View	Description
Informational	N/A	This level traps system events that are not related to sensors, such as "The host has booted."
Warning	NC	The sensor is outside of its normal range but not critical.
Critical	CT	The sensor has crossed a critical threshold.
Nonrecoverable	NR	The sensor has reached a threshold beyond the tolerance level of the corresponding components.
Disable	N/A	Do not send alerts at this level.

Examples

To configure an alert, enter:

```
-> set /SP/AgentInfo/PEF/Destination1=128.145.77.21 level=
critical
```

To change an alert level to critical, enter:

```
-> set /SP/AgentInfo/PEF/1 level=critical
```

To turn off an alert, enter:

```
-> set /SP/AgentInfo/PEF/1 level=disable
```

Displaying Information

You can display active session, current versions, and other information about the SP using the CLI.

▼ To Display Version Information

- **Enter the following command to display the current SP version:**

  ```
  version
  ```

▼ To Display Available Target Information

- **To display the available valid PEF targets, enter the following commands:**

  ```
  -> cd /SP/AgentInfo/PEF
  -> show
  ```

  The displayed PEF targets are: `EventFilterTable`[*1...6*].

  To navigate to and display the Platform Event Filter table properties, enter the following commands:

  ```
  -> cd SP/AgentInfo/PEF/EventFilterTable1
  ```

  ```
  -> show
  ```

TABLE 6-7 PEF Table Target Properties

Property	Value
status	enable | disable
sensortype	all | voltage | temperature | memory
powerctrl	PowerDown | Reset | PowerCycle
diagnosticinterrupt	enable | disable
SendAlert	enable | disable
SendMail	enable | disable

Examples

To show a specific PEF table target property for EventFilterTable1, enter:

```
-> cd /SP/AgentInfo/PEF/EventFilterTable1
-> show property
```

To enable a PEF table target property:

Set the status, by navigating to the target, and using the `set` command:

```
-> cd /SP/AgentInfo/PEF/EventFilterTable1
```

```
-> set status=enable
```

Then set the property and the value (see TABLE 6-7). For example, to set the sensortype property to the voltage value, enter the following command:

```
–> set sensortype=voltage
```

Enter the show command to display your settings:

```
–> show
```

Syntax

```
set [target=value]
```

Enter the following command to configure the platform Event Filter table properties:

```
-> set SP/AgentInfo/PEF property=value
```

TABLE 6-8 Platform Event Filter Table Properties

Property:	Value:
PEFGlobalCtrl	enable	disable
PEFActionGlobalCtrlPowerOff	enable	disable
PEFActionGlobalCtrlPowerCycle	enable	disable
PEFActionGlobalCtrlPowerReset	enable	disable
PEFActionGlobalCtrlAlert	enable	disable
PEFActionGlobalCtrlMail	enable	disable
PEFActionGlobalCtrlInterrupt	enable	disable

Examples

To show a PEF global control, enter:

```
-> cd /SP/AgentInfo/PEF/
-> show
```

To enable the PEF global power cycle, enter:

```
-> cd /SP/AgentInfo/PEF/EventFilterTable1
-> set PEFActionGlobalCtlPowerCycle=enable
```

Updating the Firmware

You can use CLI to update the SP firmware. Updating the ELOM from the command line enables you to update both the firmware, and the BIOS at the same time.

▼ To Update the Firmware

Caution – Power interruptions during the update process could leave the SP in a unbootable or nonrecoverable state. Before upgrading your firmware, ensure that you have reliable power and protect against accidental power interruptions.

Caution – The file system would become corrupted if the host operating system is not shut down before the update process begins. If the OS is running when the update process starts, the SP will shut the host down ungracefully, which could cause file system corruption.

Note – The upgrade takes about 5 minutes to complete, depending on network traffic. During this time, no other tasks can be performed in the Embedded Lights Out Manager software.

1. **Copy the combined** `bios/bmc` **image to your Tftp server.**
2. **If the server OS is running, perform a clean shutdown.**
3. **Log in to the CLI, and navigate to the TftpUpdate directory. Enter:**

```
-> cd /SP/TftpUpdate
```

Note – A network failure during the file upload will result in a timeout. This causes the SP to reboot with the prior version of the firmware.

4. **To set the IP address of the TFTP server, enter the following command:**

```
-> set ServerIP=129.148.53.204
```

5. **To set the file name of the combined** `bmc.bios` **image, enter the following command:**

```
-> set Filename=filename
```

   a. **To set the update method to overwrite existing custom settings, enter:**

   ```
   -> set Update=action
   ```

   This is the default method. It clears the CMOS, and overwrites all customized BIOS settings.

   b. **To set the update method to preserve existing custom settings, enter:**

   ```
   -> set UpdateMethod=PreserveCMOS
   ```

   This method preserves the CMOS settings.

6. **Start the tftp download:**

```
-> set Update=action
```

Example:

```
-> cd /SP/TftpUpdate
-> set ServerIPAddress=129.148.53.204
-> set FileName=filename
-> set Update=action
getting image...
getting image successfully.
prepare to update...
Prepare OK!
Update Successful
starting update...
```

CHAPTER 7

Using IPMI

This chapter describes the Intelligent Platform Management Interface (IPMI) functionality and lists the supported IPMI commands. It includes the following sections:

- "About IPMI" on page 71.
- "Supported IPMI 2.0 Commands" on page 73.

About IPMI

The Intelligent Platform Management Interface (IPMI) is an open-standard hardware management interface specification that defines a specific way for embedded management subsystems to communicate. IPMI information is exchanged through a baseboard management controller (BMC), which is located on a IPMI-compliant hardware component, such as the service processor (SP). Using low-level hardware intelligence instead of the operating system has two main benefits: first, this configuration allows for out-of-band server management, and second, the operating system is not burdened with transporting system status data.

You can manage your server with the IPMI v.1.5/2.0 on your server module or stand-alone server, which runs a daemon to do the following:

- Support low pin count (LPC) host interface in two modes:
  - KCS Mode (3 channels)
  - BT Mode (1 channel with 32 bytes of FIFO)
- Support dedicated NIC or shared lights out management (LOM)
- Support Serial-On-LAN (SOL)
- Customize FRU/Sensor Data Record data (firmware independent)
- Provide KVM over IP (remote access to the server)

- Enable the user interface (UI) for hot key definitions (for example Ctrl-Alt-Del)
- Provide full screen display switch
- Set dynamic video scaling (4x4 Video Scalar)

Your Sun Blade X6250 server module is IPMI v2.0 compliant. You can access IPMI functionality through the command line with the IPMItool utility either in-band or out-of-band. Additionally, you can generate an IPMI-specific trap from the web interface or manage the server's IPMI functions from any external management solution that is IPMI v1.5 or v2.0 compliant. For more information about the IPMI v2.0 specification, go to `http://www.intel.com/design/servers/ipmi/spec.htm#spec2`

IPMItool

IPMItool is a simple command-line interface that is useful for managing IPMI-enabled devices. You can use this utility to perform IPMI functions with a kernel device driver or over a LAN interface. IPMItool enables you to manage system field-replaceable units (FRUs), monitor system health, and monitor and manage system environmentals, independent of the operating system.

Download this tool from `http://ipmitool.sourceforge.net/`, or locate IPMItool and its related documentation on your server Resource CD.

When IPMItool is installed, it includes a man page. To view it, enter:

```
man ipmitool
```

If your client machine has a default installation of Solaris 10, you can find a preinstalled version of IPMItool in the following directory:`/usr/sfw/bin`. The binary file is called `ipmitool`.

Sensors

Your server includes a number of IPMI-compliant sensors that measure things such as voltages, temperature ranges, and security latches that detect when the enclosure is opened. For a complete list of sensors, see your platform supplement.

The sensors can activate system fault lights, and register events in the system event log (SEL). To see the system event log from the IPMItool, at the prompt, enter the following command:

ipmitool -H *ipaddress of the SP* **-U root -P** *password* **sel list**

Depending on where IPMItool is installed from, the `-P` option might be missing. In such a case, do not type the `-P` from the previous command, and enter the password when prompted.

Supported IPMI 2.0 Commands

TABLE 7-1 lists the supported IPMI 2.0 commands.

For details on individual commands, see the IPMI Intelligent Platform Management Interface Design Specification, v2.0. A copy is available at:

`http://www.intel.com/design/servers/ipmi/spec.htm`

TABLE 7-1 Supported IPMI 2.0 Commands

Supported IPMI 2.0 Commands
General Commands
Get Device ID
Cold Reset
Warm Reset
Get Self Test Results
Set/Get ACPI Power State
Reset/Set/Get Watchdog Timer
Set/Get BMC Global Enables
Clear/Get Message Flags
Enable Message Channel Receive
Get/Send Message
Read Event Message Buffer
Get Channel Authentication Capabilities
Get Session Challenge
Activate/Close Session
Set Session Privilege Level
Get Session Info
Set/Get Channel Access
Get Channel Info

TABLE 7-1 Supported IPMI 2.0 Commands *(Continued)*

Supported IPMI 2.0 Commands *(Continued)*
Set/Get User Access
Set/Get User Name
Set User Password
Master Write-Read
Set/Get Chassis Capabilities
Get Chassis Status
Chassis Control
Chassis Identify
Set Power Restore Policy
Get System Restart Cause
Set/Get System Boot Options
Set/Get Event Receiver IPMI
System Interface Support
KCS
BT
Serial Over LAN
RCMP
• Multiple Payloads
• Enhanced Authentication
• Encryption
PEF and Alerting Commands
Get PEF Capabilities
Arm PEF Postpone Timer
Set/Get PEF Configuration Parameters
Set/Get Last Processed Event ID
Alert Immediate
PET Acknowledge
Sensor Device Commands
Get Sensor Reading Factors

TABLE 7-1 Supported IPMI 2.0 Commands *(Continued)*

Supported IPMI 2.0 Commands ***(Continued)***
Set/Get Sensor Hysteresis
Set/Get Sensor Threshold
Set/Get Sensor Event Enable
Get Sensor Reading
Set Sensor Type
FRU Device Commands
Get FRU Inventory Area Info
Read/Write FRU Data SDR Device
Get SDR Repository Info
Get SDR Repository Allocation
Reserve SDR Repository
Get/Add SDR
Partial Add SDR
Clear SDR Repository
Get SDR Repository Time
Enter/Exit SDR Repository Update
Run Initialization Agent
SEL Device Commands
Get SEL Info
Get SEL Allocation Info
Reserve SEL
Get/Add SEL Entry
Clear SEL
Set/Get SEL Time
LAN Device Commands
Get LAN Configuration Parameters
Suspend BMC ARPs

TABLE 7-1 Supported IPMI 2.0 Commands *(Continued)*

Supported IPMI 2.0 Commands *(Continued)*
Serial/Modem Device Commands
Set/Get Serial Modem Configuration
Set Serial Modem MUX
Get TAP Response Codes
Serial/Modem Connection Active
Callback
Set/Get User Callback Options
Event Commands
Get Event Count
Set/Get Event Destination
Set/Get Event Reception State
Send ICMB Event Message

CHAPTER 8

Using Simple Network Management Protocol

This chapter describes how to use Simple Network Management Protocol (SNMP). It includes the following sections:

- "About SNMP" on page 77.
- "SNMP MIB Files" on page 78.
- "MIBs Integration" on page 78.
- "SNMP Messages" on page 79.
- "Configuring SNMP on the ELOM" on page 80.
- "Managing SNMP User Accounts" on page 81.

About SNMP

The Sun server supports the Simple Network Management Protocol (SNMP) interface, versions 1, 2c, and 3. SNMP is an open technology that enables the management of networks and devices, or nodes, connected to the network. SNMP messages are sent over IP using the User Datagram Protocol (UDP). Any management application that supports SNMP can manage your server.

How SNMP Works

Utilizing SNMP requires two components, a network management station and a managed node (in this case, the ELOM). Network management stations host management applications, which monitor and control managed nodes.

Managed nodes are any number of devices, including servers, routers, and hubs that host SNMP management agents responsible for carrying out the requests from management stations. The management station monitors nodes by polling management agents for the appropriate information using queries. Managed nodes can also provide unsolicited status information to a management station in the form of a trap. SNMP is the protocol used to communicate management information between the management stations and agents.

The SNMP agent is preinstalled and runs on the ELOM, so all SNMP management of the server should occur through the ELOM. To utilize this feature, your operating system must have an SNMP client application. See your operating system vendor for more information.

The SNMP agent on your ELOM provides inventory management and sensor and system state monitoring capabilities.

SNMP MIB Files

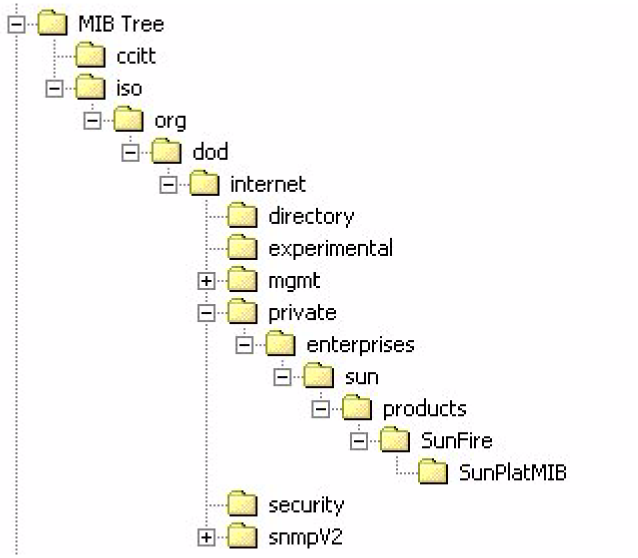
The base component of an SNMP solution is the management information base (MIB). MIB is a text file that describes a managed node's available information and where it is stored. When a management station requests information from a managed node, the agent receives the request and retrieves the appropriate information from the MIBs. The Sun server supports the following SNMP classes of management information base (MIB) files. Download and install the product-specific MIB files from your Resource CD or the Tools and Drivers CD for your platform.

- The system group and SNMP group from RFC1213 MIB
- SNMP-FRAMEWORK-MIB
- SNMP-USER-BASED-MIB
- SNMP-MPD-MIB SUN-PLATFORM-MIB
- ENTITY-MIB

MIBs Integration

Use the MIBs to integrate the management and monitoring of the server into SNMP management consoles. The MIB branch is a private enterprise MIB, located at MIB object iso(1).org (3). dod (6) .internet (1) .private (4) .enterprises (1) .sun (42) .products (2). See FIGURE 8-1. The standard SNMP port, 161, is used by the SNMP agent on the ELOM.

FIGURE 8-1 Sun Server MIB Tree



SNMP Messages

SNMP is a protocol, not an operating system, so you need some type of application to use SNMP messages. Your SNMP management software might provide this functionality, or you can use an open-source tool like net-SNMP, which is available at `http://net-snmp.sourceforge.net/`.

Both management stations and agents use SNMP messages to communicate. Management stations can send and receive information. Agents can respond to requests and send unsolicited messages in the form of a trap. There are five functions that management stations and agent, use:

- Get
- GetNext
- GetResponse
- Set
- Trap

By default, port 161 is used for SNMP messages, and port 162 is used to listen for SNMP traps.

Configuring SNMP on the ELOM

The ELOM has a preinstalled SNMP agent that supports trap delivery to an SNMP management application.

To use this feature, you must integrate the platform-specific MIBs into your SNMP environment, tell your management station about your server, then configure the specific traps.

▼ To use SNMP on the SP

This example shows how to use SNMP with a third-party MIB browser.

1. **From the Manager Preferences menu, choose Load/Unload MIBS: SNMP.**
2. **Locate and select the** `SUN-PLATFORM-MIB.mib` **file.**

   The `SUN-PLATFORM-MIB` file is available on your Tools and Drivers CD.
3. **Click Load.**
4. **Specify the directory where server MIBs are placed and click Open.**
5. **Repeat Steps 2 through 4 to load other MIBs.**
6. **Exit the Manager Preferences menu.**
7. **Open an SNMP MIB browser.**

   The SNMP standard tree appears in the MIB browser.
8. **Locate the Sun branch located under private\enterprises.**

   Verify that the SUN-PLATFORM_MIB is integrated.

Adding Your Server to Your SNMP Environment

Add your Sun server as a managed node using your SNMP management application. See your SNMP management application documentation for further details.

Configuring Receipt of SNMP Traps

Configure a trap in your ELOM. See "Managing Alerts" on page 63, or "Configuring Email Notification" on page 27.

Managing SNMP User Accounts

You can create, set permissions, delete, and modify SNMP user accounts from the CLI. By default, SNMP v3 is enabled, and SNMP v1 and v2c are disabled.

▼ To Create an SNMP User Account

This procedure details the creation of an SNMP user account. TABLE 8-1 shows the both the value and the default values for the user account properties.

1. **To navigate to the SNMP user directory, enter the following command:**

   ```
   –> cd /SP/AgentInfo/SNMP/user
   ```

2. **To create a user, enter:**

   ```
   –> create username
   ```

   username The login name of the user account.

   The above steps are used to create an SNMP v3 read-only user account. To create an SNMP v1/v2c user account enter:

   ```
   –> create /SP/AgentInfo/SNMP/communities/community_name
   ```

   community_name The name of the SNMP community you are creating.

3. **When prompted, supply the values for the following properties:**

   Applicable values are shown in TABLE 8-1.

   `AuthProtocol`
   `AuthPassword` (the system requires you to confirm the password)
   `PrivacyProtocol` (if you enter the DES protocol, you will be prompted to supply a privacy password)
   `PrivacyPassword` (the system requires you to confirm the password)

Note – If you enter an incorrect value, the create user process will fail, and you will need to start over.

After supplying values for the above properties a success message appears indicating the end of the create user process.

▼ To Set Permission for a User Account

This procedure details setting the permission level for an SNMP user account.

1. **To navigate to the user directory, enter the following command:**

   –> **`cd /SP/AgentInfo/SNMP/user`**

2. **To list users, enter:**

   –> **`show`**

   The show command allows you to identify all users.

3. **Navigate to the user's directory:**

   –> **`cd`** *username*

   username The name of the user identified in Step 2.

4. **To change the permission for a user account, use the set command. Enter:**

   –> **`set Permssion=`***value*

   value Either `ro` (read-only) or `rw` (read/write).

▼ To Delete a User Account

This procedure details deleting an SNMP user account.

1. **From the root position, enter the following command at the CLI prompt:**

   –> **`cd /SP/AgentInfo/SNMP/user`**

2. **To list users, enter:**

   –> **`show`**

   The show command allows you to identify all users.

3. **To delete a user enter the following command:**

   –> **`delete`** *username*

   username The name of the user identified in step 2.

   The above steps are used to delete an SNMP v3 read-only user account. To create an SNMP v1/v2c user account enter:

   –> **`delete /SP/AgentInfo/SNMP/communities/`***community_name*

   community_name The name of the SNMP community that you want to delete.

Modifying User Accounts

Use the `set` command to configure SNMP user accounts.

Syntax

`set target` *[propertyname***=***value]*

Targets, Properties, and Values

These targets, properties, and values are valid for SNMP user accounts.

TABLE 8-1 SNMP Targets, Properties, and Values

Target	Property	Value	Default
`/`**`SP/AgentInfo/SNMP`**`/communities/communityname`	Permissions	ro|rw	ro
`/`**`SP/AgentInfo/SNMP/user`**`/username`	AuthProtocol	MD5|SHA	MD5
	AuthPassword	*string*	(Null string)
	Permission	ro|rw	ro
	PrivacyProtocol	none|DES	None*
	PrivacyPassword	*string*	(Null string)

* If the PrivacyProtocol property has a value other than none, then PrivacyPassword must be set.

Examples

When changing the parameters of SNMP user, you must set values for all of the properties, even if you are not changing all of the values. For example, to change a user's PrivacyProtocol property to DES you must enter:

```
-> set /SP/AgentInfo/SNMP/user/username PrivacyProtocol=DES
PrivacyPassword=password AuthProtocol=SHA AuthPassword=password
```

Your changes would be invalid if you entered only:

```
-> set /SP/AgentInfo/SNMP/user/al PrivacyProtocol=DES
```

Note – You can change SNMP user permissions without resetting the privacy and authentication properties.

To show an SNMP user's properties, enter this command from the user's directory at /SP/AgentInfo/SNMP/user/*username*:

```
-> show
```

The result appear as follows:

```
/SP/AgentInfo/SNMP/user/username
     Targets:
Properties:
          Permission = ro
          AuthProtocol = SHA
          AuthPassword = (Cannot show property)
          PrivacyProtocol = DES
          PrivacyPassword = (Cannot show property)

     Target Commands:
          show
          set

/SP/AgentInfo/SNMP/user/username ->
```

APPENDIX **A**

Command-Line Interface Reference

This chapter contains the most common Embedded Lights Out Manager (ELOM) commands used to administer your Sun server from the command-line interface (CLI). This chapter contains the following sections:

- "CLI Command Quick Reference" on page 85.
- "CLI Command Reference" on page 89.
- "CLI Error Messages" on page 99

CLI Command Quick Reference

The following tables provide a quick reference to the most common ELOM CLI commands.

TABLE A-1 Command Syntax and Usage

Content	Typeface	Description
Your input	**`Fixed-width bold`**	Text that you type at the computer. Enter it in exactly as shown.
Onscreen output	`Fixed-width regular`	Text that the computer displays.
Variable	*Italic*	Replace these with a name or value you choose.
Square brackets, [ ]		Text in square brackets is optional.
Vertical bars, |		Text separated by a vertical bar represents the only available values. Select one.

TABLE A-2 General Commands

Description	Command
Log out of the CLI.	`exit`
Display the version of the ELOM firmware running on the SP.	`version`
Display information about commands and targets.	`help`
Display information about a specific command.	`help` *command or target*

TABLE A-3 User Commands

Description	Command
Add a local user.	**`create /SP/users/`***username* (user names must be between 8-16 characters in length)
Set or change password.	**`set /SP/users/`***username* **`password=`***xxxx* (passwords must be between 8-16 characters in length)
Set or change permission.	**`set /SP/users/`***username* **`permission=`** **`operator|administrator|callback|user`** (the default is operator)
Delete a local user.	**`delete /SP/users/`***username*
Change a local user's properties.	**`set /SP/users/`***username* **`permission=operator`**
Display information about all local users.	**`show -display [`**targets|properties|all**`]`** **`-level [`***value*|*all***`] /SP/users`**

TABLE A-4 Network and Serial Port Setting Commands

Description	Command
Display network configuration information.	**`show /SP/network`**
Change network properties for the ELOM. Changing certain network properties, like the IP address, will disconnect your active session. You cannot change the MACaddress.	**`set /SP/network`** **`IPAddress`**=*xxx.xxx.xxx.xxx* **`Netmask=`***xxx.xxx.xxx.xxx* **`Gateway=`***xxx.xxx.xxx.xxx*
Set DHCP or change to static settings.	**`set /SP/network IPSource=[`***dhcp*|*static***`]`**

TABLE A-5 Alert Commands

Description	Command
Display information about PET alerts.	**show /SP/AgentInfo/PET/Destination***[1...4]*
Change alert configuration.	**set /SP/AgentInfo/PET/ Destination***[1...4]* **IPAdress=** *ipaddress*

TABLE A-6 SNMP Commands

Description	Command
Display information about SNMP settings. By default, the SNMP port is 161, and v3 is enabled.	**show /SP/AgentInfo/SNMP**
	show /SP/AgentInfo/SNMP port=*snmpportnumber* **snmpset=***enabled*|*disabled*
Display SNMP users.	**show /SP/AgentInfo/SNMP/user**
Add an SNMP user.	**create /SP/AgentInfo/SNMP/user/***snmpusername* **authpassword=***password* **authprotocol=[**MD5|SHA] **permission=**rw|ro **privacypassword=***password* **privacyprotocol=**none|DES
Delete an SNMP user.	**delete /SP/services/SNMP/user/***snmpusername*
Display information about SNMP public (read-only) communities.	**show /SP/AgentInfo/SNMP/communities/public**
Add this device to an SNMP public community.	**create /SP/AgentInfo/SNMP/communities/ public/***comm1*
Delete this device from an SNMP public community.	**delete /SP/AgentInfo/SNMP/communities/ public/***comm1*

TABLE A-6 SNMP Commands

Description	Command
Display information about SNMP private (read-write) communities.	**show /SP/AgentInfo/SNMP/communities/private**
Add this device to an SNMP private community.	**create /SP/AgentInfo/SNMP/communities/ private/***comm2*
Delete this device from an SNMP private community.	**delete /SP/AgentInfo/NMP/communities/ private/***comm2*

TABLE A-7 System Start and Stop Commands

Description	Command
Start the host system.	**set /SP/SYS/CtrlInfo PowerCtrl=on**
Stop the host system gracefully.	**set /SP/SYS/CtrlInfo PowerCtrl=gracefuloff**
Stop the host system forcefully.	**set /SP/SYS/CtrlInfo PowerCtrl=forceoff**
Reset the host system.	**set /SP/SYS/CtrlInfo PowerCtrl=reset**
Start a session to connect to the host console.	**start /SP/AgentInfo/console**
Stop the session connected to the host console.	**stop /SP/AgentInfo/console**

CLI Command Reference

This section provides reference information about the CLI commands.

cd

Use the `cd` command to navigate the namespace. When you use `cd` to change to a target location, that location then becomes the default target for all other commands.

Using the - `default` option with no target returns you to the top of the namespace. Entering just `cd` displays your current location in the namespace. Entering `help targets` displays a list of all targets in the entire namespace.

Syntax

`cd` *target*

Options

`[-h|help]`

Targets and Properties

Any location in the namespace.

Examples

To create a user named newuser1, use `cd` to change to `/SP/users`, then execute the `create` command with `/SP/users` as the default target.

```
-> cd /SP/users
```

```
-> create newuser1
```

To return to the root position, enter:

```
-> cd /
```

create

Use the `create` command to set up an object in the namespace. Unless you specify properties with the `create` command, they are empty.

Syntax

`create [`*options*`] target [`*propertyname=value*`]`

Options

`[-h|help]`

Targets, Properties, and Values

TABLE A-8 Create command Targets, Properties, Values, and Defaults

Valid Targets	Properties	Values	Default
`/SP/users/`*username*	password role	*string* [administrator | operator | user | callback]	(None) operator
`/SP/AgentInfo/SNMP/communities/`*communityname*	permissions	[ro | rw]	ro
`/SP/AgentInfo/SNMP/user/`*username*	authenticationprotocol authenticationpassword permissions privacyprotocol privacypassword	MD5 *string* [ro | rw] [none | DES] *string*	MD5 (Null string) ro DES (Null string)

Example

```
-> create /SP/users/susan role=administrator
```

delete

Use the `delete` command to remove an object from the namespace. You are not prompted to confirm a `delete` command.

Syntax

`delete [`*options***`]`** *target*

Options

`[-h|help]`

Targets

TABLE A-9 `delete` Command Targets

Valid Targets
`/SP/users/`*username*
`/SP/AgentInfo/SNMP/communities/`*communityname*
`/SP/AgentInfo/SNMP/user/`*username*

Example

```
-> delete /SP/users/basicuser
```

exit

Use the `exit` command to terminate a session to the CLI.

Syntax

`exit [`*options***`]`**

Options

[-h|help]

help

Use the `help` command to display Help information about commands and targets. Using the `-output terse` option displays usage information only. The **-**`output verbose` option displays usage, description, and additional information including examples of command usage. If you do not use the `-output` option, usage information and a brief description of the command are displayed.

Specifying `command` targets displays a complete list of valid targets for that command from the fixed targets in `/SP`. Fixed targets are targets that cannot be created by a user.

Syntax

help *command*

Options

[-h|help]

Commands

cd, create, delete, exit, help, load, reset, set, show, start, stop, version

Example

```
-> help load

The load command is used to transfer a file from a server and update
a target.
Usage: load -source URL targets
Available options for this command:
-help : display help message of this command
```

set

Use the `set` command to change the value of a property associated with a target.

Syntax

`set [target] property=value [`*propertyname*`=`*value*`]`

Options

`[-h help]`

Targets, Properties, and Values

TABLE A-10 `set` Command Targets, Properties, and Values

Valid Targets	Properties	Values	Default
`/SP/users/`*username*	password	*string*	(None)
	permission	[administrator | operator | user | callback]	operator
`/SP/clock`	Date	MM/DD/CCYY	/SP/clock
	Time	hh/mm/ss	
`/SP/AgentInfo/SNMP`	port	*decimal*	161
	snmpset	[enabled | disabled]	disabled
	version1	[enabled | disabled]	disabled
	version2c	[enabled | disabled]	disabled
	version3	[enabled | disabled]	enabled

TABLE A-10 `set` Command Targets, Properties, and Values *(Continued)*

Valid Targets	Properties	Values	Default
`/SP/AgentInfo/SNMP communities/`*communityname*	Permissions	[ro|rw]	ro
`/SP/AgentInfo/SNMP/user /`*username*	AuthProtocol	[MD5|SHA]	MD5
	AuthPassword	*string*	(Null string)
	Permission	[ro|rw]	ro
	PrivacyProtocol	[none|DES]	DES
	PrivacyPassword	*string*	(Null string)
`/SP/network`	IPAddress	[*IP address*|none]	(None)
	Netmask	[*IP address*|none]	255.255.255.255
	Gateway	[*IP address*|none]	(None)
	DNS	*[IP address*|none]	(None)
	IPSource	[dhcp|static]	(None)
	Hostname	*STRING*	

Example

```
-> set /SP/users/basicuser permission=administrator
```

show

Use the `show` command to display information about targets and properties.

The `show` command is used to display information about managed elements. It can be used to view information about a single managed elements, a tree of managed elements, or managed elements matching a property value filter.

The `-level` option controls the depth of the `show` command, and it applies to all modes of the `-display` option. Specifying `-level 1` displays the level of the namespace where the object exists. Values greater than 1 return information for the target's current level in the namespace and the *specified value* levels below. If the argument is `-level all`, it applies to the current level in the namespace and everything below.

Syntax

```
show [options] [-display targets|properties|commands|all] [-l1
-level 1|2|3...|all] [target] [property property...]
```

Options

[-d|display] [-h|-help] [-l|level]

Targets and Properties

TABLE A-11 show Command Targets and Properties

Valid Targets	Properties
/SP/network	MACaddress
	IPAddress
	Netmask
	Gateway
	DNS
	IPSource
	Hostname

Examples

```
->show /SP/network

  /SP/network


Targets:
    Target Commands:
        show
        set
```

start

Use the `start` command to turn on the target or to initiate a connection to the host console.

Syntax

start [options] target

Options

[-h|help]

Targets

TABLE A-12 `start` Command Target

Valid Target	Description
/SP/AgentInfo/Console	Starts an interactive session to the console stream.

Examples

```
-> start /SP/AgentInfo/Console
```

stop

Use the `stop` command to shut down the target or to terminate another user's connection to the host console.

Syntax

```
stop [options] target
```

Options

[-h|help]

Targets

TABLE A-13 `stop` Command Target

Valid Target	Description
`/SP/AgentInfo/Console`	Terminate another user's connection to the host console.

Examples

```
-> stop /SP/AgentInfo/Console
```

reset

Use the `reset` command to reset the target's state. This command can be used with and without options.

Syntax

reset [*target*]

Options

[-h|help]

Example

```
-> reset /system3
```

version

Use the `version` command to display ELOM version information.

Syntax

version

Options

[-h|help]

Example

```
-> version
```

```
SM CLP Version v1.0.0

SM ME Addressing Version v1.0.0
```

CLI Error Messages

Verbs

cd

Error Message	Description
Current default target: *current path*	Did not specify target
cd: invalid target *target path*	Target node does not exist, invalid path

create

Error Message	Description
create: Parent object does not exist	Parent node does not exist
create: Object cannot be created	Do not specify target name
create failed	Cannot create a node

delete

Error Message	Description
delete: invalid target *target path*	Invalid target or do not specify target name
delete: Object *target path* cannot be deleted	Invalid target

exit

Error Message	Description
exit: sytax error, the exit command does not support a target.	Did not support exit

help

Error Message	Description
help: Invalid command *input string* - type help for a list of commands.	Input string does not match any name in command list
help: Invalid command syntax Usage: help [-o | -output terse | verbose] [<command> | legal | targets]	Too many parameter

reset

Error Message	Description
reset: invalid target *target path*	Invalid target or do not specify target name
reset: Object *target path* cannot be reset	Invalid target

set

Error Message	Description
set: syntax error	if no any argument, this is command syntax error
set: invalid target *input token*	User input more than one token at first time.
set: invalid property *input token*	Input token is not a property
set: object *input token* cannot be written	Input token is only readable
Could not set *node name* to *input value string*	Set fail

Targets

show

Error Message	Description
show: invalid target *target path*	Input invalid target path

start

Error Message	Description
start: invalid target *target path*	Invalid target or do not specify target name
start: Object *target path* cannot be started	Invalid target

stop

Error Message	Description
stop: invalid target *target path*	Invalid target or do not specify target name
stop: Object *target path* cannot be stopped	Invalid target
console de-activate successful	Not specify examine option, do it actually

version

Version	
Error Message	**Description**
Invalid syntax, the version command does not support a target.	Do not support version command.

/SP/users

Error Message	Description
Maximum number of users exceeded.	Maximum number of users exceeded.
Password should be more than 8 character and less than 20 characters.	Password rule
Username and Password can not be the same.	User rule
Every character of password only can be 0-9 a-z A-z.	Password rule
Inconsistent passwords entered.	Password rule
create: target name must only contain alphabets and digits	Username rule
create: target name should be lower case	Username rule
create: invalid arguments	Username rule

/SP/network

/SP/network

Error Message	Description
Could not be modified under DHCP.	User should turn off DHCP flag before setting IP, Net mask, DNS and Gateway.
Invalid IP	Invalid IP

/SP/clock

Error Message	Description
set: bad parameter *date and time string*	Wrong format of date and time.

/SP/TftpUpdate and /SP/CPLDUpdate

Error Message	Description
Invalid filename.	Invalid filename.
cannot get ip	Cannot get ip
Cannot get file	Cannot get file
Cannot get save flag	Cannot get save flag
Please DC off.	Alert user to turn DC off before updating.
Update environment has something wrong, please check IP, Filename and Saveflag.	Need to check tftp update IP Filename or Saveflag.
Could not update.	Maybe someone has done updating.
Getting image fail.	Cannot upload image to server.
BIOS progress file cannot be found.	Cannot find BIOS progress file.
wrong parameter.	Should set update=action
Could not get correct update mode from config file.	Setting of tftp update has something wrong.

Set server IP fail.	Set tftp or cpld IP address fail.
Set source file fail.	Set tftp or cpld filename address fail.
Set save configuration fail.	Set tftp or cpld save flag address fail.
Update environment has something wrong, please check IP and Filename.	Setting of cpld update has something wrong.

/SP/AgentInfo/PEF and /SP/AgentInfo/PET

Error Message	Description
Get PEF fail	Get PEF fail
Incorrect Parameter	Incorrect Parameter
Need to enable status first	User should enable status before setting PEF event table.
Set PEF fail	Set PEF fail

/SP/AgentInfo/SEL

Error Message	Description
IPMI open failure	Cannot connect with bmc
IPMI request failure	Cannot get information from bmc

/SP/AgentInfo/Mail

Error Message	Description
IPMI read failure	Reading information from bmc fail.
IPMI write failure	Setting information to bmc fail.
Parameter cannot be empty and should less than 64 bits	Mail address string should be between 1 to 64 characters
Please input correct Email format	Email format is wrong.

/SP/AgentInfo/SNMP

Error Message	Description
Could not get snmp community info.	Could not get snmp community info.
Could not add snmp community.	Could not add snmp community.

/SP/AgentInfo/Console

Error Message	Description
No response query console	No response
Error: Select returned with nothing to read	Returned with nothing to read
Error in console session	Console session closed abnormally

/SYS/BoardInfo/
/SYS/ProductInfo/
/SYS/ChassisInfo/
/SYS/CPU/
/SYS/Fan/
/SYS/Temperature/
/SYS/Voltage

Error Message	Description
IPMI open fail	Cannot connect with BMC
Cannot get FRU data	Cannot get FRU data

/SYS/CtrlInfo/

Error Message	Description
IPC read fail	Read Boot Option fail
wrong variable	Set wrong variable

APPENDIX **B**

U.S. Keyboard Map

Use these U.S. keyboard map figures to convert key combinations.

FIGURE B-1 U.S. Keyboard (Detail)

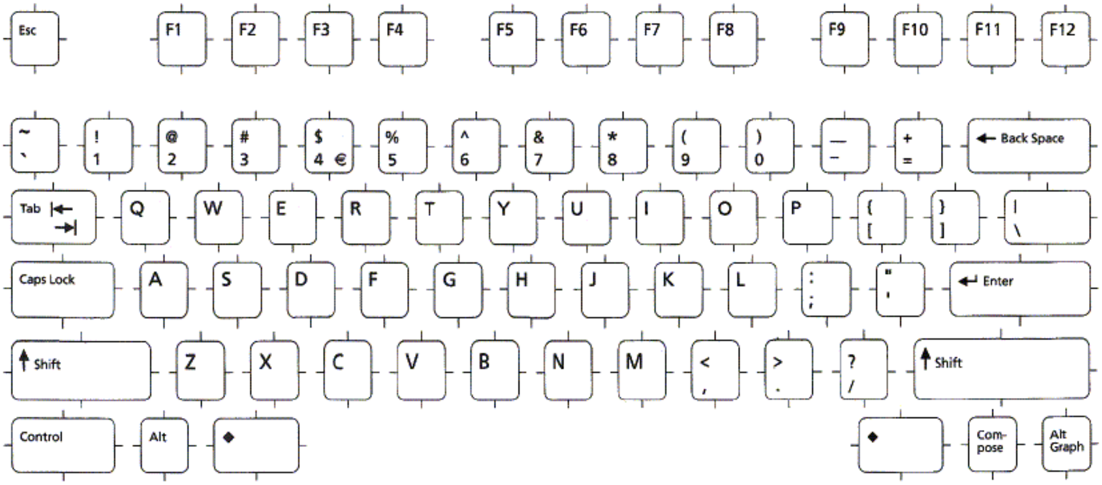
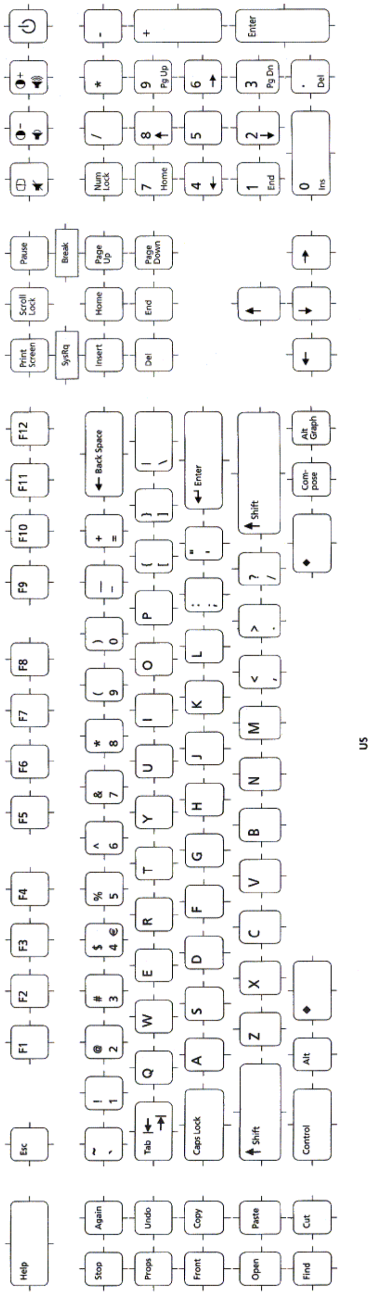


FIGURE B-2 U.S. Keyboard (Full)


Help
Stop Again
Props Undo
Front Copy
Open Paste
Find Cut
Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12
~ ` ! 1 @ 2 # 3 $ 4 € % 5 ^ 6 & 7 * 8 (9) 0 _ - + = Back Space
Tab Q W E R T Y U I O P { [}] | \
Caps Lock A S D F G H J K L : ; " ' Enter
Shift Z X C V B N M < , > . ? / Shift
Control Alt ◆ ◆ Com-pose Alt Graph
Print Screen SysRq Scroll Lock Pause Break
Insert Home Page Up
Del End Page Down
Num Lock / * -
7 Home 8 9 Pg Up +
4 5 6
1 End 2 3 Pg Dn Enter
0 Ins . Del
US

Glossary

The following terms are used within the Sun server documentation.

A

access control list (ACL) A software authorization mechanism that enables you to control which users have access to a server. Users can define ACL rules that are specific to a particular file or directory, granting or denying access to one or more users or groups.

address In networking, a unique code that identifies a node in the network. Names such as "host1.sun.com" are translated to dotted-quad addresses like "168.124.3.4" by the domain name service (DNS).

address resolution A means for mapping Internet addresses into physical media access control (MAC) addresses or domain addresses.

Address Resolution Protocol (ARP) A protocol used to associate an Internet Protocol (IP) address with a network hardware address (MAC address).

Administrator The person with full access (root) privileges to the managed host system.

Advanced Configuration and Power Interface (ACPI) An open-industry specification that provides power management capabilities to a system that enables the operating system to determine when peripheral devices are idle and to utilize ACPI-defined mechanisms for putting the devices into low power modes. The ACPI specification also describes a large number of power states for CPUs, devices, and systems as a whole. One feature of the ACPI enables the OS to modify the voltage and frequency of a

CPU in response to system load, thus enabling the system's main power-consuming element (the CPU) to vary its power consumption based on system load.

Advanced Programmable Interrupt Controller (APIC) A device that manages interrupt requests for multiple central processing units (CPUs). The APIC decides which request has the highest priority and sends an interrupt to the processor for that request.

Advanced Technology Attachment (ATA) A specification that describes the physical, transport, electrical, and command protocols used to attach storage devices to host systems.

Advanced Technology Attachment Packet Interface (ATAPI) An extension to the Advanced Technology Attachment (ATA) standard for connecting removable media storage devices in host systems, including CD/DVD drives, tape drives, and high-capacity diskette drives. Also called "ATA-2" or "ATA/ATAPI."

agent A software process, usually corresponding to a particular local managed host, that carries out manager requests and makes local system and application information available to remote users.

alert A message or log generated by the collection and analysis of error events. An alert indicates that there is a need to perform some hardware or software corrective action.

Alert Standard Format (ASF) A preboot or out-of-band platform management specification that enables a device, such as an intelligent Ethernet controller, to autonomously scan ASF-compliant sensors on the motherboard for voltage, temperature, or other excursions and to send Remote Management and Control Protocol (RMCP) alerts according to the Platform Event Trap (PET) specification. ASF was intended primarily for out-of-band management functions for client desktops. ASF is defined by the Distributed Management Task Force (DMTF).

authentication The process that verifies the identity of a user in a communication session, or a device or other entity in a computer system, before that user, device, or other entity can access system resources. Session authentication can work in two directions. A server authenticates a client to make access control decisions. The client can authenticate the server as well. With Secure Sockets Layer (SSL), the client always authenticates the server.

authorization The process of granting specific access privileges to a user. Authorization is based on authentication and access control.

AutoYaST An installation program for SUSE Linux that automates the process of configuring one or more servers.

B

bandwidth A measure of the volume of information that can be transmitted over a communication link. Often used to describe the number of bits per second a network can deliver.

baseboard management controller (BMC) A device used to manage chassis environmental, configuration, and service functions, and receive event data from other parts of the system. It receives data through sensor interfaces and interprets this data by using the sensor data record (SDR) to which it provides an interface. The BMC provides another interface to the system event log (SEL). Typical function of the BMC is to measure processor temperature, power supply values, and cooling fan status. The BMC can take autonomous action to preserve system integrity. The BMC is also known as the service processor (SP).

baud rate The rate at which information is transmitted between devices, for example, between a terminal and a server.

bind In the Lightweight Directory Access Protocol (LDAP), refers to the authentication process that LDAP requires when users access the LDAP directory. Authentication occurs when the LDAP client binds to the LDAP server.

BIOS (Basic Input/Output System) System software that controls the loading of the operating system and testing of hardware at system power-on. BIOS is stored in read-only memory (ROM).

bits per second (bps) The unit of measurement for data transmission speed.

boot loader A program contained in read-only memory (ROM) that automatically runs at system power-on to control the first stage of system initialization and hardware tests. The boot loader then transfers control to a more complex program that loads the operating system.

C

cache A copy of original data that is stored locally, often with instructions or the most frequently accessed information. Cached data does not have to be retrieved from a remote server again when requested. A cache increases effective memory transfer rates and processor speed.

certificate Public key data assigned by a trusted Certificate Authority (CA) to provide verification of an entity's identity. This is a digitally signed document. Both clients and servers can have certificates. Also called a "public key certificate."

Certificate Authority (CA) A trusted organization that issues public key certificates and provides identification to the owner of the certificate. A public key Certificate Authority issues certificates that state a relationship between an entity named in the certificate and a public key that belongs to that entity, which is also present in the certificate.

client In the client-server model, a system or software on a network that remotely accesses resources of a server on a network.

command-line interface (CLI) A text-based interface that enables users to enter executable instructions at a command prompt.

Common Information Model (CIM) An open systems information model published by the Distributed Management Task Force (DMTF) that enables a common application to manage disparate resources, such as printers, disk drives, or CPUs.

console A terminal or dedicated window on a screen where system messages are displayed. The console window enables you to configure, monitor, maintain, and troubleshoot many server software components.

Coordinated Universal Time (UTC) The international standard for time. UTC was formerly called Greenwich Meridian Time (GMT). UTC is used by Network Time Protocol (NTP) servers to synchronize systems and devices on a network.

core file A file created by the Solaris or Linux operating system when a program malfunctions and terminates. The core file holds a snapshot of memory, taken at the time the fault occurred. Also called a "crash dump file."

critical event A system event that seriously impairs service and requires immediate attention.

custom JumpStart™ A type of installation in which the Solaris software is automatically installed on a system that is based on a user-defined profile.

customer-replaceable unit (CRU) A system component that the user can replace without special training or tools.

D

Data Encryption Standard (DES) A common algorithm for encrypting and decrypting data.

Desktop Management Interface (DMI) A specification that sets standards for accessing technical support information about computer hardware and software. DMI is hardware and operating system (OS) independent, and can manage workstations, servers, or other computing systems. DMI is defined by the Distributed Management Task Force (DMTF).

digital signature A certification of the source of digital data. A digital signature is a number derived from a public key cryptographic process. If the data is modified after the signature was created, the signature becomes invalid. For this reason, a digital signature can ensure data integrity and detection of data modification.

Digital Signature Algorithm (DSA) A cryptographic algorithm specified by the Digital Signature Standard (DSS). DSA is a standard algorithm used to create digital signatures.

direct memory access (DMA) The transfer of data directly into memory without supervision of the processor.

directory server In the Lightweight Directory Access Protocol (LDAP), a server that stores and provides information about people and resources within an organization from a logically centralized location.

disk array A storage subsystem containing an arrangement of multiple disk drives, designed to provide performance, high availability, serviceability, and other benefits.

disk partition A logical section of a physical hard disk drive reserved for a specific file system and function.

Distinguished Name (DN) In the Lightweight Directory Access Protocol (LDAP), a unique text string that identifies an entry's name and location within the directory. A DN can be a fully qualified domain name (FQDN) that includes the complete path from the root of the tree.

Distributed Management Task Force (DMTF) A consortium of over 200 companies that authors and promotes standards for the purpose of furthering the ability to remotely manage computer systems. Specifications from the DTMF include the Desktop Management Interface (DMI), the Common Information Model (CIM), and the Alert Standard Format (ASF).

domain A grouping of hosts that is identified by a name. The hosts usually belong to the same Internet Protocol (IP) network address. The domain also refers to the last part of a fully qualified domain name (FQDN) that identifies the company or organization that owns the domain. For example, “sun.com” identifies Sun Microsystems as the owner of the domain in the FQDN “docs.sun.com.”

domain name The unique name assigned to a system or group of systems on the Internet. The host names of all the systems in the group have the same domain name suffix, such as “sun.com.” Domain names are interpreted from right to left. For example, “sun.com” is both the domain name of Sun Microsystems, and a subdomain of the top-level “.com” domain.

domain name server (DNS) The server that typically manages host names in a domain. DNS servers translate host names, such as “www.example.com,” into Internet Protocol (IP) addresses, such as “030.120.000.168.”

domain name service (DNS) The data query service that searches domains until a specified host name is found.

domain name system (DNS) A distributed name resolution system that enables computers to locate other computers on a network or the Internet by domain name. The system associates standard Internet Protocol (IP) addresses, such as “00.120.000.168,” with host names, such as “www.sun.com.” Machines typically get this information from a DNS server.

dual inline memory module (DIMM) A circuit board that holds double the amount of surface-mount memory chips that a single inline memory module (SIMM) holds. A DIMM has signal and power pins on both sides of the board, whereas a SIMM has pins on only one side of the board. A DIMM has a 168-pin connector and supports 64-bit data transfer.

Dynamic Host Configuration Protocol (DHCP) A protocol that enables a DHCP server to assign Internet Protocol (IP) addresses dynamically to systems on a Transmission Control Protocol/Internet Protocol (TCP/IP) network.

dynamic random access memory (DRAM) A type of random access memory (RAM) that stores information in integrated circuits that contain capacitors. Because capacitors lose their charge over time, DRAM must be periodically recharged.

E

electrically erasable programmable read-only memory (EEPROM) A type of nonvolatile programmable read-only memory (PROM) that can be erased by being exposed to an electrical charge.

electrostatic discharge (ESD) The sudden dissipation of static electrical charge. ESD can easily destroy semiconductor components.

Embedded Lights Out Manager (ELOM) A dedicated system of hardware and supporting software that enables you to manage your Sun server using several interfaces, independent of the operating system, and under various power conditions.

enhanced parallel port (EPP) A hardware and software standard that enables systems to transmit data at twice the speed of standard parallel ports.

erasable programmable read-only memory (EPROM) A nonvolatile programmable read-only memory (PROM) that can be written to as well as read from.

Ethernet An industry-standard type of local area network (LAN) that enables real-time communication between systems connected directly through cables. Ethernet uses a Carrier Sense Multiple Access/Collision Detection (CSMA/CD) algorithm as its access method, wherein all nodes listen for, and any node can begin transmitting, data. If multiple nodes attempt to transmit at the same time (a collision), the transmitting nodes wait for a random amount of time before attempting to transmit again.

event A change in the state of a managed object. The event-handling subsystem can provide a notification to which a software system must respond when it occurs, but which the software did not solicit or control.

externally initiated reset (XIR) A signal that sends a "soft" reset to the processor in a domain. XIR does not reboot the domain. An XIR is generally used to escape from a hung system to reach the console prompt. You then can generate a core dump file, which can be useful in diagnosing the cause of the hung system.

F

failover The automatic transfer of a computer service from one system, or more often a subsystem, to another to provide redundant capability.

Fast Ethernet Ethernet technology that transfers data up to 100 Mbit/sec. Fast Ethernet is backward compatible with 10Mbit per second Ethernet installations.

fdisk partition A logical partition of a physical disk drive that is dedicated to a particular operating system on an x86-based system.

Fibre Channel (FC) A connector that provides high bandwidth, increased distance, and additional connectivity from hosts to peripherals.

Fibre Channel-Arbitrated Loop (FCAL) A 100-Mbyte per second loop topology used with Fibre Channel that enables connection of multiple devices such as disk drives and controllers. An arbitrated loop connects two or more ports, but enables only two ports to communicate at a given time.

field-replaceable unit (FRU) A system component that is replaceable at the customer site.

file system A consistent method by which information is organized and stored on physical media. Different operating systems typically have different file systems. File systems are often a tree-structured network of files and directories, with a root directory at the top and parent and child directories below the root.

File Transfer Protocol (FTP) A basic Internet protocol based on Transmission Control Protocol/Internet Protocol (TCP/IP) that enables the retrieving and storing of files between systems on the Internet without regard to the operating systems or architectures of the systems involved in the file transfer.

firewall A network configuration, usually both hardware and software, that protects networked computers within an organization from outside access. A firewall can monitor or prohibit connections to and from specified services or hosts.

firmware Software that is typically used to help with the initial booting stage of a system and with system management. Firmware is embedded in read-only memory (ROM) or programmable ROM (PROM).

flash PROM Programmable read-only memory (PROM) that can be reprogrammed while installed within the system, from software on a disc, by a voltage pulse, or flash of light.

fully qualified domain name (FQDN) The complete and unique Internet name of a system, such as "www.sun.com." The FQDN includes a host server name (www) and its top-level (.com) and second-level (.sun) domain names. A FQDN can be mapped to a system's Internet Protocol (IP) address.

G

gateway A computer or program that interconnects two networks and then passes data packets between the networks. A gateway has more than one network interface.

Gigabit Ethernet Ethernet technology that transfers data up to 1000 Mbit/sec.

Grand Unified Bootloader (GRUB) A boot loader that can install two or more operating systems (OS) onto a single system and that can manage which OS to boot at power-on.

graphical user interface (GUI) An interface that uses graphics, along with keyboard and mouse, to provide easy-to-use access to an application.

H

heatsink A structure, attached to or part of a semiconductor device, that can dissipate heat to the surrounding environment.

host A system, such as a back-end server, with an assigned Internet Protocol (IP) address and host name. The host is accessed by other remote systems on the network.

host ID Part of the 32-bit Internet Protocol (IP) address used to identify a host on a network.

host name The name of a particular machine within a domain. Host names always map to a specific Internet Protocol (IP) address.

hot plug Describes a component that is safe to remove or add while the system is running. Typically, the system must be rebooted before the hot-pluggable component is configured into the system.

hot swap Describes a component that you can install or remove by simply pulling the component out and putting a new component into a running system. The system either automatically recognizes the component change and configures it, or requires user interaction to configure the system. However, in neither case is a reboot required. All hot-swappable components are hot-pluggable components, but not all hot-pluggable components are hot-swappable components.

Hypertext Transfer Protocol (HTTP) The Internet protocol that retrieves hypertext objects from remote hosts. HTTP messages consist of requests from client to server and responses from server to client. HTTP is based on Transmission Control Protocol/Internet Protocol (TCP/IP).

Hypertext Transfer Protocol Secure (HTTPS) An extension of HTTP that uses Secure Sockets Layer (SSL) to enable secure transmissions over a Transmission Control Protocol/Internet Protocol (TCP/IP) network.

I

in-band system management Server management capability that is enabled only when the operating system is initialized and the server is functioning properly.

install server A server that provides the Solaris software DVD or CD images from which other systems on a network can install the Solaris software.

Integrated Lights Out Manager (ILOM) An integrated hardware, firmware, and software solution for in-chassis or in-blade system management.

Intelligent Platform Management Interface (IPMI) A hardware-level interface specification that was designed primarily for out-of-band management of server systems over a number of different physical interconnects. The IPMI specification describes extensive abstractions regarding sensors, enabling a management application running on the operating system (OS) or in a remote system to comprehend the environmental makeup of the system and to register with the system's IPMI subsystem to receive events. IPMI is compatible with management software from heterogeneous vendors. IPMI functionality includes FRU inventory reporting, system monitoring, logging, system recovery (including local and remote system resets and power on and off capabilities), and alerting.

Internet Control Message Protocol (ICMP) An extension to the Internet Protocol (IP) that provides for routing, reliability, flow control, and sequencing of data. ICMP specifies error and control messages used with the IP.

Internet Protocol (IP) The basic network layer protocol of the Internet. IP enables the unreliable delivery of individual packets from one host to another. IP does not guarantee that the packet will be delivered, or how long it will take, or if multiple packets will be delivered in the order they were sent. Protocols layered on top of IP add connection reliability.

Internet Protocol (IP) address In Transmission Control Protocol/Internet Protocol (TCP/IP), a unique 32-bit number that identifies each host or other hardware system on a network. The IP address is a set of numbers separated by dots, such as "192.168.255.256," that specifies that actual location of a machine on an intranet or the Internet.

interrupt request (IRQ) A signal that a device requires attention from the processor.

IPMItool A utility used to manage IPMI-enabled devices. IPMItool can manage IPMI functions of either the local system or a remote system. Functions include managing field-replaceable unit (FRU) information, local area network (LAN) configurations, sensor readings, and remote system power control.

J

Java Web Start application A web application starter. With Java Web Start, you start applications by clicking the web link. If the application is not present on your system, Java Web Start downloads it and caches it onto your system. Once an application is downloaded to its cache, it can be started from a desktop icon or browser link. The most current version of the application is always presented.

JumpStart installation A type of installation in which the Solaris software is automatically installed on a system by using the factory-installed JumpStart software.

K

kernel The core of the operating system (OS) that manages the hardware and provides fundamental services, such as filing and resource allocation, that the hardware does not provide.

Keyboard Controller Style (KCS) interface A type of interface implemented in legacy personal computer (PC) keyboard controllers. Data is transferred across the KCS interface using a per-byte handshake.

keyboard, video, mouse, storage (KVMS) A series of interfaces that enables a system to respond to keyboard, video, mouse, and storage events.

L

lights out management (LOM) Technology that provides the capability for out-of-band communication with the server even if the operating system is not running. This enables the system administrator to switch the server on and off; view system temperatures, fan speeds, and so forth; and restart the system from a remote location.

Lightweight Directory Access Protocol (LDAP) A directory service protocol used for the storage, retrieval, and distribution of information, including user profiles, distribution lists, and configuration data. LDAP runs over Transmission Control Protocol/Internet Protocol (TCP/IP) and across multiple platforms.

Lightweight Directory Access Protocol (LDAP) server A software server that maintains an LDAP directory and service queries to the directory. The Sun Directory Services and the Netscape Directory Services are implementations of an LDAP server.

Linux Loader (LILO) A boot loader for Linux.

local area network (LAN) A group of systems in close proximity that can communicate via connecting hardware and software. Ethernet is the most widely used LAN technology.

local host The processor or system on which a software application is running.

M

major event A system event that occurred that impairs service, but not seriously.

management information base (MIB) A tree-like, hierarchical system for classifying information about resources in a network. The MIB defines the variables that the master Simple Network Management Protocol (SNMP) agent can access. The MIB provides access to the server's network configuration, status, and statistics. Using SNMP, you can view this information from a network management station (NMS). By industry agreement, individual developers are assigned portions of the tree structure to which they may attach descriptions that are specific to their own devices.

man pages Online UNIX documentation.

media access control (MAC) address Worldwide unique, 48-bit, hardware address number that is programmed into each local area network interface card (NIC) at the time of manufacture.

Message Digest 5 (MD5) A secure hashing function that converts an arbitrarily long data string into a short digest of data that is unique and of fixed size.

minor event A system event that occurred that does not currently impair service, but which needs correction before it becomes more severe.

N

namespace In the tree structure of a Lightweight Directory Access Protocol (LDAP) directory, a set of unique names from which an object name is derived and understood. For example, files are named within the file namespace, and printers are named within the printer namespace.

network file system (NFS) A protocol that enables disparate hardware configurations to function together transparently.

Network Information Service (NIS) A system of programs and data files that UNIX systems use to collect, collate, and share specific information about machines, users, file systems, and network parameters throughout a network of computer systems.

network interface card (NIC) An internal circuit board or card that connects a workstation or server to a networked device.

network management station (NMS) A powerful workstation with one or more network management applications installed. The NMS is used to remotely manage a network.

network mask A number used by software to separate the local subnet address from the rest of a given Internet Protocol (IP) address.

node An addressable point or device on a network. A node can connect a computing system, a terminal, or various peripheral devices to the network.

nonmaskable interrupt (NMI) A system interrupt that is not invalidated by another interrupt.

nonvolatile memory A type of memory that ensures that data is not lost when system power is off.

nonvolatile random access memory (NVRAM) A type of random access memory (RAM) that retains information when system power is off.

O

object identifier (OID) A number that identifies an object's position in a global object registration tree. Each node of the tree is assigned a number, so that an OID is a sequence of numbers. In Internet usage the OID numbers are delimited by dots, for example, "0.128.45.12." In the Lightweight Directory Access Protocol (LDAP), OIDs are used to uniquely identify schema elements, including object classes and attribute types.

OpenBoot™ PROM A layer of software that takes control of an initialized system after the power-on self-test (POST) successfully tests components. OpenBoot PROM builds data structures in memory and boots the operating system.

OpenIPMI An operating system-independent, event-driven library for simplifying access to the Intelligent Platform Management Interface (IPMI).

operator A user with limited privileges to the managed host system.

out-of-band (OOB) system management Server management capability that is enabled when the operating system network drivers or the server is not functioning properly.

P

parity A method used by a computer for checking that data received matches data sent. Also refers to information stored with data on a disk that enables the controller to rebuild data after a drive failure.

partition A physical section on a hard disk drive.

Peripheral Component Interconnect (PCI) A local bus standard used to connect peripherals to 32-bit or 64-bit systems.

Peripheral Interface Controller (PIC) An integrated circuit that controls peripherals in an interrupt request (IRQ)–driven system, taking away that load from the central processing unit (CPU).

permissions A set of privileges granted or denied to a user or group that specify read, write, or execution access to a file or directory. For access control, permissions state whether access to the directory information is granted or denied, and the level of access that is granted or denied.

physical address An actual hardware address that matches a memory location. Programs that refer to virtual addresses are subsequently mapped to physical addresses.

platform event filter (PEF) A mechanism that configures the service processor to take selected actions when it receives event messages, for example, powering off or resetting the system or triggering an alert.

Platform Event Trap (PET) A configured alert triggered by a hardware or firmware (BIOS) event. A PET is an Intelligent Platform Management Interface (IPMI)–specific, Simple Network Management Protocol (SNMP) trap, which operates independently of the operating system.

port The location (socket) to which Transmission Control Protocol/Internet Protocol (TCP/IP) connections are made. Web servers traditionally use port 80, the File Transfer Protocol (FTP) uses port 21, and Telnet uses port 23. A port enables a client program to specify a particular server program in a computer on a network. When a server program is started initially, it binds to its designated port number. Any client that wants to use that server must send a request to bind to the designated port number.

port number A number that specifies an individual Transmission Control Protocol/Internet Protocol (TCP/IP) application on a host machine, providing a destination for transmitted data.

power cycling The process of turning the power to a system off then on again.

power-on self-test (POST) A program that takes uninitialized system hardware and probes and tests its components at system startup. POST configures useful components into a coherent, initialized system and hands it over to the OpenBoot PROM. POST passes to OpenBoot PROM a list of only those components that have been successfully tested.

PowerPC An embedded processor.

Preboot Execution Environment (PXE) An industry-standard client–server interface that enables a server to boot an operating system (OS) over a Transmission Control Protocol/Internet Protocol (TCP/IP) network using Dynamic Host Configuration Protocol (DHCP). The PXE specification describes how the network adapter card and BIOS work together to provide basic networking capabilities for the primary bootstrap program, enabling it to perform a secondary bootstrap over the network, such as a TFTP load of an OS image. Thus, the primary bootstrap program, if coded to PXE standards, does not need knowledge of the system's networking hardware.

Privacy Enhanced Mail (PEM) A standard for Internet electronic mail that encrypts data to ensure privacy and data integrity.

programmable read-only memory (PROM) A memory chip on which data can be programmed only once and which retains the program forever. PROMs retain data even when power is off.

protocol A set of rules that describes how systems or devices on a network exchange information.

proxy A mechanism whereby one system acts on behalf of another system in responding to protocol requests.

public key encryption A cryptographic method that uses a two-part key (code) that is made up of public and private components. To encrypt messages, the published public keys of the recipients are used. To decrypt messages, the recipients use their unpublished private keys, which are known only to them. Knowing the public key does not enable users to deduce the corresponding private key.

R

rack unit (U) A measure of vertical rack space equal to 1.75 inches (4.45 cm).

random access memory (RAM) Volatile, semiconductor-based memory in which any byte of memory can be accessed without touching the preceding bytes.

read-only file A file that a user cannot modify or delete.

read-only memory (ROM) A nonvolatile memory chip on which data has been prerecorded. Once written onto a ROM chip, data cannot be removed and can only be read.

real-time clock (RTC) A battery-backed component that maintains the time and date for a system, even when the system is powered off.

reboot An operating system–level operation that performs a system shutdown followed by a system boot. Power is a prerequisite.

Red Hat Package Manager (RPM) A collection of tools developed by Red Hat, Inc. for Red Hat Linux that can automate the install, uninstall, update, verify, and query software processes on a computer. RPM is now commonly used by many Linux vendors.

redirection The channeling of input or output to a file or device rather than to the standard input or output of a system. The result of redirection sends input or output that a system would normally display to the display of another system.

redundant array of independent disks (RAID) A way of storing the same data at different places, thus redundantly, on multiple hard disks. RAID enables a set of disk drives to appear as a single logical disk drive to an application such as a database or file system. Different RAID levels provide different capacity, performance, high availability, and cost characteristics.

Remote Management and Control Protocol (RMCP) A networking protocol that enables an administrator to respond to an alert remotely by powering the system on or off, or forcing a reboot.

remote procedure call (RPC) A method of network programming that enables a client system to call functions on a remote server. The client starts a procedure at the server, and the result is transmitted back to the client.

remote system A system other than the one on which the user is working.

reset A hardware-level operation that performs a system power-off, followed by a system power-on.

root In UNIX operating systems, the name of the superuser (root). The root user has permissions to access any file and carry out other operations not permitted to ordinary users. Roughly equivalent to the Administrator user name on Windows Server operating systems.

root directory The base directory from which all other directories stem, either directly or indirectly.

router A system that assigns a path over which to send network packets or other Internet traffic. Although both hosts and gateways do routing, the term "router" commonly refers to a device that connects two networks.

RSA algorithm A cryptographic algorithm developed by RSA Data Security, Inc. It can be used for both encryption and digital signatures.

S

schema Definitions that describe what type of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory might be unable to display the proper results.

Secure Shell (SSH) A UNIX shell program and network protocol that enables secure and encrypted login and execution of commands on a remote system over an insecure network.

Secure Sockets Layer (SSL) A protocol that enables client-to-server communication on a network to be encrypted for privacy. SSL uses a key exchange method to establish an environment in which all data exchanged is encrypted with a cipher and hashed to protect it from eavesdropping and alteration. SSL creates a secure connection between a web server and a web client. Hypertext Transfer Protocol Secure (HTTPS) uses SSL.

sensor data record (SDR) To facilitate dynamic discovery of features, the Intelligent Platform Management Interface (IPMI) includes this set of records that include software information such as how many sensors are present, what type they are, their events, threshold information, and so forth. The sensor data records enable software to interpret and present sensor data without any prior knowledge about the platform.

Serial Attached SCSI (SAS) A point-to-point serial peripheral interface that links controllers directly to disk drives. SAS devices include two data ports that enable failover redundancy, which guarantees data communication through a separate path.

serial console A terminal or a tip line connected to the serial port on the service processor. A serial console is used to configure the system to perform other administrative tasks.

server certificate A certificate used with Hypertext Transfer Protocol Secure (HTTPS) to authenticate web applications. The certificate can be self-signed or issued by a Certificate Authority (CA).

Server Message Block (SMB) protocol A network protocol that enables files and printers to be shared across a network. The SMB protocol provides a method for client applications to read and write to files on, and to request services from, server programs in the network. The SMB protocol enables you to mount file systems between Windows and UNIX systems. The SMB protocol was designed by IBM and subsequently modified by Microsoft Corp. Microsoft renamed the protocol the "Common Internet File System (CIFS)."

service processor (SP) A device used to manage chassis environmental, configuration, and service functions, and receive event data from other parts of the system. It receives data through sensor interfaces and interprets this data by using the sensor data record (SDR) to which it provides an interface. The SP provides another interface to the system event log (SEL). Typical function of the SP is to measure processor temperature, power supply values, and cooling fan status. The SP can take autonomous action to preserve system integrity.

session timeout A specified duration after which a server can invalidate a user session.

Simple Mail Transfer Protocol (SMTP) A Transmission Control Protocol/Internet Protocol (TCP/IP) used for sending and receiving email.

Simple Network Management Protocol (SNMP) A simple protocol used to exchange data about network activity. With SNMP, data travels between a managed device and a network management station (NMS). A managed device can be any device that runs SNMP, such as hosts, routers, web servers, or other servers on the network.

Small Computer System Interface (SCSI) An ANSI standard for control of peripheral devices by one or more host computers. SCSI defines a standard I/O bus-level interface and a set of high-level I/O commands.

Spanning Tree Protocol (STP) A networking protocol based on an intelligent algorithm that enables bridges to map a redundant topology and eliminates packet looping in local area networks (LANs).

subnet A working scheme that divides a single logical network into smaller physical networks to simplify routing. The subnet is the portion of an Internet Protocol (IP) address that identifies a block of host IDs.

subnet mask A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Also called an “address mask.”

superuser A special user who has privileges to perform all administrative functions on a UNIX system. Also called “root.”

system event log (SEL) A log that provides nonvolatile storage for system events that are logged autonomously by the service processor, or directly with event messages sent from the host.

T

Telnet The virtual terminal program that enables the user of one host to log in to a remote host. A Telnet user of one host who is logged in to a remote host can interact as a normal terminal user of the remote host.

threshold Minimum and maximum values within a range that sensors use when monitoring temperature, voltage, current, and fan speed.

timeout A specified time after which the server should stop trying to finish a service routine that appears to be hung.

transmission control block (TCB) Part of the Transmission Control Protocol/Internet Protocol (TCP/IP) that records and maintains information about the state of a connection.

Transmission Control Protocol/Internet Protocol (TCP/IP) An Internet protocol that provides for the reliable delivery of data streams from one host to another. TCP/IP transfers data between different types of networked systems, such as systems running Solaris, Microsoft Windows, or Linux software. TCP guarantees delivery of data and that packets will be delivered in the same sequence in which they were sent.

trap Event notification made by Simple Network Management Protocol (SNMP) agents by their own initiative when certain conditions are detected. SNMP formally defines seven types of traps and permits subtypes to be defined.

Trivial File Transport Protocol (TFTP) A simple transport protocol that transfers files to diskless systems. TFTP uses User Datagram Protocol (UDP).

U

uninterruptible power supply (UPS) An auxiliary or backup power supply that provides electrical service over extended system power outages. A UPS for a LAN or computer system provides continuous power in the event of a power failure.

Universal Serial Bus (USB) An external bus standard that supports data transfer rates of 450 Mbit/sec. (USB 2.0). A USB port connects devices, such as mouse devices, keyboards, modems, and printers to the computer system.

unshielded twisted pair/shielded twisted pair (UTP/STP) A type of Ethernet cable.

user account A record of essential user information that is stored on the system. Each user who accesses a system has a user account.

User Datagram Protocol (UDP) A connectionless, transport layer protocol that adds some reliability and multiplexing to the Internet Protocol (IP). UDP enables one application program to deliver, via IP, datagrams to another application program on another machine. The Simple Network Management Protocol (SNMP) is usually implemented over UDP.

user identification (userID) A unique string identifying a user to a system.

user identification number (UID number) The number assigned to each user accessing a UNIX system. The system uses UID numbers to identify, by number, the owners of files and directories.

user name A combination of letters, and possibly numbers, that identifies a user to the system.

V

voltage regulator module (VRM) An electronic device that regulates a system's microprocessor voltage requirements to maintain the correct voltage.

volume One or more disk drives that can be grouped into a unit for data storage.

volume manager Software that organizes data blocks on physical disk drives into logical volumes, which makes the disk data independent of the physical path name of the disk drives. Volume manager software provides data reliability through disk striping, concatenation, mirroring, and dynamic growth of metadevices or volumes.

W

W3C Refers to the World Wide Web Consortium. W3C is an international organization that governs Internet standards.

web server Software that provides services to access the Internet or an intranet. A web server hosts web sites, provides support for HTTP/HTTPS and other protocols, and executes server-side programs.

wide area network (WAN) A network consisting of many systems that provides file transfer services. A WAN can cover a large physical area, sometimes worldwide.

X

X.509 certificate The most common certificate standard. X.509 certificates are documents containing a public key and associated identity information, digitally signed by a Certificate Authority (CA).

X Window System A common UNIX window system that enables a workstation or terminal to control multiple sessions simultaneously.

Index