

Dell™ PowerEdge™
Systems

Using the Baseboard Management Controller

Notes, Cautions, and Warnings



NOTE: A NOTE indicates important information that helps you make better use of your computer.

Information in this document is subject to change without notice.
© 2011 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell and the DELL logo are trademarks of Dell Inc.; Microsoft, Windows, and Internet Explorer are registered trademarks of Microsoft Corporation; Linux is the registered trademark of Linus Torvalds; Java is a registered trademark of Sun Microsystems, Inc. or its subsidiaries in the United States and other countries. Intel is a registered trademark of Intel Corporation in the U.S. and other countries.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

Contents

Intelligent Platform Management Interface	5
Baseboard Management Controller	5
BMC Key Features and Functions	5
Watchdog and Automatic System Recovery	6
Virtual Storage	6
Using the Web User Interface	6
Logging into the Web User Interface	6
Remote Management Controller	7
Logging into the Web User Interface	6
Remote Management Controller	7
System Information	7
Server Health	8
Configuration	8
Remote Control	12
Maintenance	13
Languages	15
Updating Firmware Using the TFTP Flash Interface	15
Running Virtual Media	16
Connecting and Disconnecting Virtual Media	16
JViewer Menu	17
IPMI 2.0 Command Support Lis	18
Chassis Control Command Implementation	37
Entity ID and Instance Table	38
Sensor Summary	39
Threshold Settings and Converting Formulas	43
Power Throttling Function	46
Power Throttling Configuration in BIOS Setup Utility	47
Additional Power Throttling Information	47
Power Throttling Protection	47
Information From the Fan Control Board	47
Extended Configurations	48
Appendix	53
SSH/Telnet Enable and Disable	53

SSH/Telnet Enable and Disable	54
VLAN ID	55
BMC/BIOS Version Information.	56
BIOS Version Information	57

Intelligent Platform Management Interface

The Intelligent Platform Management Interface (IPMI) defines a set of standardized, message-based interfaces that monitor system hardware health (fan speed, temperature, voltage, power supply, etc.), control system components, and store data about important system events in a system event log (SEL) for later examination. IPMI provides the foundation for remote platform management.

Baseboard Management Controller

The key component in the IPMI system is the baseboard management controller (BMC), a microcontroller located in the server's motherboard. BMC is the "intelligence" within the IPMI architecture, responsible for monitoring and controlling the system's manageable devices.

The BMC is connected to the various sensors through the Intelligent Platform Management Bus (IPMB), a subset of the I2C bus. System software communicates with BMC using a keyboard controller style (KCS) interface.

BMC Key Features and Functions

Following are the supported features of the BMC:


- IPMI v2.0.
- Out-of-band monitoring and control for server management over LAN.
- Dedicated 10/100 NIC for remote management over a network.
- Information report including main board part number, product name, manufacturer, etc.
- Health status/hardware monitoring report.
- Events log, view, and clear.
- Event notification using chassis LED indicator and Platform Event Trap (PET).
- Platform Event Filtering (PEF) to take selected action for selected events, including non-masking interrupt (NMI) and system management interrupt (SMI).
- Chassis management including power control and status report, front panel buttons, LED control, Secure Mode, and Boot Option.
- Watchdog and auto server re-start and recovery.
- Multi-session user and alert destination for LAN channel.
- IPMB connector to enable advanced server management communication with BMC.
- DCMI v1.0/Node Manager v1.5.

Watchdog and Automatic System Recovery

The BMC watchdog timer commands, as defined in the IPMI v2.0 specification, are part of the Intelligent Platform Management Interface. The watchdog timer can restart, turn off, or cycle power to your server in your absence to support automatic system recovery functions. If a

pre-set interval expires, the configured timer actions are executed and logged into SEL for later examination. The timer commands are:

- System reset
- System power off
- System power cycle
- Host diagnostic interrupt


 **NOTE:** The software that acquired and activated the watchdog timer is responsible for resetting the timer countdown.

Virtual Storage

The firmware supports USB diskette, keyboard, mouse, and CD/DVD. These are supported as a composite device. The USB keyboard and mouse traffic is bridged to the KVM connections.


Using the Web User Interface

The embedded console client provides KVM/IP functionality. The client is in the form of an ActiveX control for the Windows[®] platform and an application for the Linux[®] platform.

 **NOTE:** The application must be installed before completing the console redirection.

A web-based graphic user interface (GUI) is supported on the following browsers:

- Windows platforms: Internet Explorer[®] 6.0 or later
- All platforms: Firefox 2.0017 or later


 **NOTE:** Before using the Web user interface, ensure that the firewall settings are configured to enable access to the following: KVM:7578, USB-CDROM:5120, and USB-Floppy:5123.

Logging into the Web User Interface

Enter the BMC-embedded server IP address or URL into the address bar of the web browser. The BMC interface has a default of (DHCP\Static). Press the <F2> key to enter the system BIOS setup and change these settings.

Remote Management Controller

The first time you access the Dell™ Remote Management Controller, you are prompted to enter a user name and password. Use “root” as the default value for both.

 **NOTE:** When you log in using the “root” user name and password, you have full administrative privileges. It is suggested that you change the user name and password after signing in for the first time.

The remote management controller offers six menu selections: System Information, Server Health, Configuration, Remote Control, Maintenance, and Languages.

System Information



The System Information menu selection allows you to:

- View system information (System Information option).
- Obtain field replaceable unit (FRU) information (List FRU option).

Table 1-1. System Information Option

BMC Information	Description
System Power Status	On or Off
Firmware Revision	Revision
Number AuxFirmware Revision	Revision
Number	
Build Time	Date firmware was last built in the format: Month Day Year HH:MM:SS

Table 1-2. List FRU Option

Chassis Information	Board Information	Product Information	
Type	Manufacturer	Manufacturer Name	Part Number
Part Number	Product Name	Product Name	Asset Tag
Serial Number	Serial Number	Serial Number	
	Part	Number	

Server Health

The Server Health menu selection allows you to:

- View system hardware information such as fan speed, internal temperature, and voltage (Sensor Readings and Sensor Readings with Thresholds buttons).
- View system event information such as event ID, time stamp, sensor name, sensor type, and description (Event Log button). This system event log is generated by the BMC or BIOS on the managed system.

Table 1-3. Server Health Options

Button	Options	Description
Sensor Readings category	Select a sensor type (drop-down list)	Select all sensors, or select a category (temperature sensors, voltage sensors, fan sensors, etc.).
	Refresh (button)	Reread the sensor state.
	Show Thresholds (button)	View the sensor readings with thresholds.
Sensor Readings with Thresholds		View the sensor readings with thresholds.
Event Log category	Select an event log (drop-down list)	Select a category (BMC generated events, BIOS generated events, etc.).
	Time Zone (radio button)	Select a time zone: local or Greenwich Mean Time (GMT).
	Clear Event Log (button)	Clear the SEL.

Configuration

The Configuration menu selection allows you to:

- Manage alert messages for platform events, such as environmental warnings or component failures (Alerts button).
- Set the mouse mode for either a Windows or Linux OS (Mouse Mode button).
- View and modify network settings (Network button).

- Set the email server IP address for sending alert notifications (SMTP button).
- View information, configure existing BMC users, and control access privileges (Users button).

Alerts

To set up a destination to receive alerts, complete these steps:

- 1 In the List of Alerts window, select an alert number and click the Modify button.

The screenshot shows the MEGARAC Aster Configuration web interface. The top navigation bar includes 'System Information', 'Server Health', 'Configuration', 'Remote Control', 'Maintenance', and 'Languages'. The main content area is titled 'Configuration' and contains a 'List of Alerts' section. Below the title, there is a table with 15 entries. The table has three columns: 'Alert #', 'Alert Level', and 'Destination Address'. All 'Alert Level' values are 'Disable All' and all 'Destination Address' values are 'Not Configured'. At the bottom of the table, there are 'Modify' and 'Delete' buttons.

Alert #	Alert Level	Destination Address
1	Disable All	Not Configured
2	Disable All	Not Configured
3	Disable All	Not Configured
4	Disable All	Not Configured
5	Disable All	Not Configured
6	Disable All	Not Configured
7	Disable All	Not Configured
8	Disable All	Not Configured
9	Disable All	Not Configured
10	Disable All	Not Configured
11	Disable All	Not Configured

- 2 In the Modify Alert window, complete the following:
 - a From the Alert Type drop-down list, select an alert type.
 - b From the Event Severity drop-down list, select a severity level.
 - c If the Alert Type is Snmp Trap, enter a destination IP.
If the Alert Type is Email, enter an email address, then enter the email subject in the Subject field.

The screenshot shows a 'Modify Alert' dialog box. It has a title bar with the text 'Modify Alert'. Below the title bar is a subtitle: 'Enter the information for the alert below and press Save.' The main area of the dialog contains several input fields. The first is 'Alert Type' with a dropdown menu showing 'Snmp Trap' selected. The second is 'Event Severity' with a dropdown menu showing 'Snmp Trap' and 'Email' options. The third is 'Destination IP' with a text box containing '0.0.0.0'. The fourth is 'Email Address' with an empty text box. The fifth is 'Subject' with an empty text box. The sixth is 'Message' with an empty text box. At the bottom of the dialog are two buttons: 'Save' and 'Cancel'.

- 3 Click the Save button.

Mouse Mode

Click the appropriate radio button to select the mouse mode, then click the Save button.

- Set Mode to Absolute—Use for Windows OS host system.
- Set Mode to Relative—Use for Linux OS host system.

Network

Click the appropriate radio button to modify network settings, then click the Save button.

SMTP

Enter the IP address for the SMTP mail server and click the Save button.

Users

The User List window displays the current list of configured users and allows you to add, modify, or delete a user.


 **NOTE:** This option is only available if you have Configure Users permission.



Table 1-4. User List Window

Column	Description
User ID	Sequential user ID
number. User Name	User login name.
Network Privilege	Privilege level to which the user is assigned (administrator, operator, user, custom, or none).

To add a user, complete these steps:

- 1 From the User List window, select an unconfigured user ID number and click the Add User button.
- 2 Enter a user name, select an IPMI version, enter and confirm a password, and select network privileges. Click the Add button.

To change the settings for a user, complete these steps:

- 1 From the User List window, select the user's ID number and click the Modify User button.
- 2 Change the applicable information and click the Modify button.

To delete a user, select the user's ID number from the User List window and click the Delete User button.

Remote Control

The Remote Control menu selection allows you to:

- Power on, power off, power cycle, and reset the system remotely (Power Control button).
- Use the local management station's display, mouse, and keyboard to control the corresponding devices on a remotely managed system (Console Redirection button).

Power Control

To perform a power control operation, click the applicable radio button, then click the Perform Action button.

Table 1-5. Power Control Options

Radio Button	Description
Reset Server	Reboot server without powering off (warm boot).
Power Off Server – Immediate	Powers off the server.
Power Off Server – Orderly Shutdown	Shuts down the server.
Power On Server	Powers on the server.
Power Cycle Server	Powers off, then reboots the server (cold boot).

Console Redirection

The most powerful feature of the Dell Remote Management Controller is the ability to redirect the host system’s console, managing the host system as though it were physically in front of you. Note the following about console redirection:

- You can run a maximum of four simultaneous redirection sessions.
- The Java[®] Video Viewer (version 1.5.15 or later) is required to run the console redirection. If the BMC detects that the video viewer is not installed, you are prompted to install it.
- The recommended display resolution on the management station is at least 1280 x 1024 pixels at 60Hz with 32 bit color. If the resolution does not meet this minimum, you will be unable to view the console in full screen mode.
- Before using console redirection, verify that your mouse mode is correct. See “Mouse Mode”.

To start a remote console session from the Console Redirection window, click the Java Console button. This launches the redirection console via the JViewer Java applet. For further information on remote console sessions, see “Running Virtual Media”.

Maintenance

The Maintenance menu selection allows you to upgrade to the latest firmware version through the GUI. The following data is included in the BMC firmware package:

- Compiled BMC firmware code and data
- Web-based user interface, JPEG, and other user interface data files
- Default configuration files



NOTE: The firmware update retains the current BMC settings.



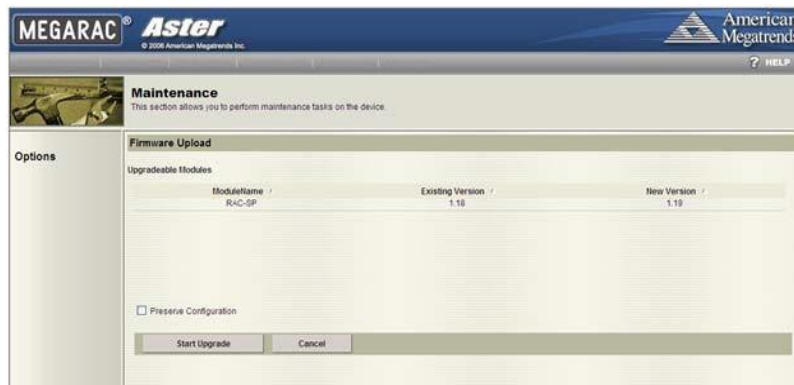
NOTE: You can also update the firmware using trivial file transfer protocol (TFTP). See “Updating Firmware Using the TFTP Flash Interface”.

Updating the BMC Firmware Through the GUI

Before beginning the firmware update, download the latest firmware version and save it on your local system. During the update, the AC power of the managed system cannot be turned off, and the GUI cannot be closed.

To update the firmware, follow these steps:

- 1 Click the Maintenance button to access the Firmware Update window.
- 2 Click the Enter Update Mode button.
- 3 Use the Select Firmware to Upload field to indicate the location of the firmware image. Either browse to the location or enter the path. For example:
C:\Updates\V1.0*image_name*
- 4 To force an update, click the Force Update checkbox. This forces the BMC to update the image without first validating the target board, target product, and version number.
- 5 Click the Upload Firmware button.
- 6 A window appears with a message indicating that the firmware image has been verified and compared to the existing device firmware. Click the OK button.
- 7 The Preserve Configuration checkbox is selected by default. If you do not wish to preserve configuration, click the checkbox to deselect it. Click the Start Upgrade button.



- 8 A window appears with a message indicating that clicking the OK button will start the upgrade. Click the button to start the operation.

- 9 When the upgrade is complete, the following message appears.



Languages

The Languages menu option allows you to select language support for multiple clients simultaneously. Select an available language from the list and click the Apply button.

Updating Firmware Using the TFTP Flash Interface

To update the firmware through the TFTP flash interface, use the IPMItool (Linux, V1.8.11).

- TFTP server IP address is 192.168.1.2
- BMC IP address is 192.168.1.1
- URI path is tftp://192.168.1.2/BMC106T1.ROM

Complete these steps:

- 1 Set up the extended configuration ID 0x10 parameters.
 - a Get a reservation ID by typing the appropriate command.
For example:

```
ipmitool -H 192.168.1.1 -U root -P root raw 0x30 0x01.
```


The response is 01. This is the reservation ID, which is used in the next command.
 - b Set the URI path of the image file by typing the appropriate command.
For example:

```
ipmitool -H 192.168.1.1 -U root -P root raw 0x30 0x03 0x01  
0x10 0x03 0x00 0x00 0x00 0x01 0x1f 0x74 0x66 0x74 0x70 0x3a  
0x2f 0x2f 0x31 0x39 0x32 0x2e 0x31 0x36 0x38 0x2e 0x31 0x2e  
0x32 0x2f 0x35 0x34 0x34 0x32 0x4d 0x31 0x30 0x30 0x2e 0x52  
0x4f 0x4d.
```


The response is 1f.

- 2 Start the firmware update through TFTP by typing the appropriate command.

For example:

```
ipmitool -H 192.168.1.1 -U root -P root raw 0x08 0x01 0x01 0x00
0x01.
```

The response is 48 (task ID).

Running Virtual Media

The console redirection feature gives the managed server access to media connected to a remote system on the network. The combination of virtual media and console redirection enables administrators to perform tasks on the server without being physically present.

The two virtual media types are:

- Optical Drive—Includes CDROM and ISO image files.
- Floppy Drive—Includes diskette/USB drives and diskette images.

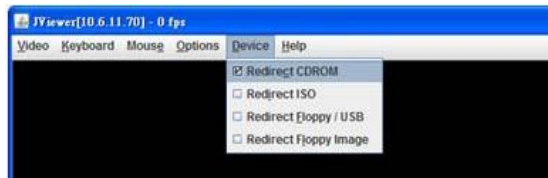
For each media type, you can virtualize one drive at a time. This may require that you disconnect media before connecting to a different source.



NOTE: You must have Access Virtual Media permission to virtualize or disconnect a drive.

Connecting and Disconnecting Virtual Media

Connect to media through the Device menu in the JViewer (see“Console Redirection” for directions for accessing the JViewer). Check the box next to the applicable media type(s).



If you are connecting to a diskette or ISO image, either browse to or enter the path where the image file resides on your system.



NOTE: Virtual device drive letters on the managed server do not correspond to physical drive letters on the management station.

To disconnect media, deselect the applicable checkbox.

JViewer Menu

The JViewer menu provides access to additional functions, outlined in the following tables.

Table 1-6. Video Menu Items

Menu Option	Description
Start Redirection	Begin console redirection.
Stop Redirection	Stop console redirection.
Restart	Stop and then restart console redirection.
Full Screen mode.	View the console redirection in full screen mode.
Exit	Exit console redirection.

Table 1-7. Keyboard Menu Items

Menu Option	Description
Hold Right Ctrl Key	Apply the right <Ctrl> key to the next keystroke sent to the remote system.
Hold Right Alt Key	Apply the right <Alt> key to the next keystroke sent to the remote system.
Hold Left Ctrl Key	Apply the left <Ctrl> key to the next keystroke sent to the remote system.
Hold Left Alt Key	Apply the left <Alt> key to the next keystroke sent to the remote system.
Left Windows Key	Select Hold Down before typing characters you want to combine with the left Windows key. Select Press and Release to send a left Windows key keystroke.
Right Windows Key	Select Hold Down before typing characters you want to combine with the right Windows key. Select Press and Release to send a right Windows key keystroke.
Alt+Ctrl+Del	Send the <Ctrl><Alt><Delete> key combination to the remote system.
Full Keyboard	Direct client keyboard functions to the server.

Table 1-8. Mouse Menu Items

Menu Option	Description
Sync Cursor	Synchronize the local cursor with the remote cursor. The remote client's cursor and the server's cursor appear together onscreen.
Single Cursor	Disable the remote client's cursor and view only the server's cursor. This resolves the issue of the remote mouse not working correctly under LSI 8708EM2 WebBIOS.

Table 1-9. Options Menu Items

Menu Options	Description
Bandwidth	Regulate the network bandwidth
setting. Video Settings	Adjust the video resolution.

IPMI 2.0 Command Support List

The following tables include all commands defined in the IPMI v2.0 specifications. All mandatory commands and some optional functions are supported. Special functions beyond the scope of IPMI v2.0 are implemented as original equipment manufacturer (OEM) commands.

In the O/M column:

M = Mandatory in the IPMI spec and is implemented.

O = Optional command supported in this implementation.

N = Not supported in this implementation.

Table 1-10. IPMI Device Global and Broadcast Commands (NETFUN: 06H, 07H)

Commands	NetFn	CMD	O/M	Supported
Get Device ID	App	01H	M	Yes
Cold Reset	App	02H	O	Yes
Warm Reset	App	03H	N	No
Get Self Test Results	App	04H	M	Yes
Manufacture Test On	App	05H	O	Yes
Set ACPI Power State	App	06H	O	Yes
Get ACPI Power State	App	07H	O	Yes
Get Device GUID	App	08H	O	Yes
Broadcast Commands:				
Broadcast 'Get Device ID'	App	01H	N	No

Table 1-11. BMC Messaging Support Commands (NETFUN: 06H, 07H)

Commands	NetFn	CMD	O/M	Supported
Set BMC Global Enables	App	2EH	M	Yes
Get BMC Global Enables	App	2FH	M	Yes
Clear Message Buffer Flags	App	30H	M	Yes

Table 1-12. BMC Messaging Support Commands (NETFUN: 06H, 07H)

Commands	NetFn	CMD	O/M	Supported
Get Message Buffer Flags	App	31H	M	Yes
Enable Message Channel Receive	App	32H	O	Yes
Get Message	App	33H	M	Yes
Send Message	App	34H	M	Yes
Read Event Message Buffer	App	35H	O	Yes
Get System Interface Capabilities	App	57H	M	Yes
Get BT Interface Capabilities	App	36H	M	No
Master Write-Read	App	52H	M	Yes
Get System GUID	App	37H	O	Yes
Set System Info Parameters	App	58H	O	Yes
Get System Info Parameters	App	59H	O	Yes
Get Channel Authentication Capabilities	App	38H	O	Yes
Get Channel Cipher Suites	App	54H	M	Yes
Get Session Challenge	App	39H	O	Yes
Activate Session	App	3AH	O	Yes
Set Session Privilege Level	App	3BH	O	Yes
Close Session	App	3CH	O	Yes
Get Session Information	App	3DH	O	Yes
Get Authentication Code	App	3FH	O	Yes
Set Channel Access	App	40H	O	Yes
Get Channel Access	App	41H	O	Yes
Get Channel Info	App	42H	O	Yes
Set Channel Security Keys	App	56H	M	Yes
Set User Access	App	43H	O	Yes
Get User Access	App	44H	O	Yes
Set User Name	App	45H	O	Yes
Get User Name	App	46H	O	Yes
Set User Password	App	47H	O	Yes

Table 1-13. Firmware, Firewall and Discovery Commands (NETFUN: 06H, 07H)

Commands	NetFn	CMD	O/M	Supported
Get NetFn Support	App	9H	N	No
Get Command Support	App	AH	N	No
Get Command Sub-function Support	App	BH	N	No
Get Configurable Commands	App	CH	N	No
Get Configurable Command Sub-functions	App	DH	N	No
Set Command Enables	App	60H	N	No
Get Command Enables	App	61H	N	No
Set Command Sub-function Enables	App	62H	N	No
Get Command Sub-function Enables	App	63H	N	No
Get OEM NetFn IANA Support	App	64H	N	No

Table 1-14. RMCP+ Support and Payload Commands (NETFUN: 06H, 07H)

Commands	NetFn	CMD	O/M	Supported
Active Payload	App	48H	M	Yes
Deactivate Payload	App	49H	M	Yes
Suspend/Resume Payload Activation Status	App	55H	M	Yes
Get Payload Activation Status	App	4AH	M	Yes
Get Payload Instance Info	App	4BH	M	Yes
Set User Payload Access	App	4CH	M	Yes
Get User Payload Access	App	4DH	M	Yes
Get Channel Payload Support	App	4EH	M	Yes
Get Channel Payload Version	App	4FH	M	Yes
Get Channel OEM Payload Info	App	50H	M	Yes

Table 1-15. IMPI LAN Commands (NETFUN: 0CH, 0DH)

Commands	NetFn	CMD	O/M	Supported
Set LAN Configuration	Transport	01H	M	Yes
Parameters Get LAN	Transport	02H	M	Yes
Configuration Parameters	Transport	03H	O	Yes
Suspend BMC ARP	Transport	04H	N	No
Get IP/UDP/RMCP				

Table 1-16. IMPI Serial/Modem Commands (NETFUN: 0CH, 0DH)

Commands	NetFn	CMD	O/M	Supported
Set Serial/Modem Configuration	Transport	10H	N	No
Get Serial/Modem Configuration	Transport	11H	N	No
Set Serial/Modem Mux	Transport	12H	N	No
Get Tap Response Codes	Transport	13H	N	No
Set PPP UDP Proxy Transmit Data	Transport	14H	N	No
Get PPP UDP Proxy Transmit Data	Transport	15H	N	No
Send PPP UDP Proxy Packet	Transport	16H	N	No
Get PPP UDP Proxy Receive Data	Transport	17H	N	No
Serial/Modem Connection Active	Transport	18H	N	No
Callback	Transport	19H	N	No
Set User Callback Options	Transport	1AH	N	No
Get User Callback Options	Transport	1BH	N	No

Table 1-17. SOL Commands (NETFUN: 0CH, 0DH)

Commands	NetFn	CMD	O/M	Supported
SOL Activating	Transport	20H	M	Yes
Set SOL Configuration Parameters	Transport	21H	M	Yes
Get SOL Configuration Parameters	Transport	22H	M	Yes

Table 1-18. BMC Watchdog Timer Commands (NETFUN: 06H, 07H)

Commands	NetFn	CMD	O/M	Supported
Reset Watchdog Timer	App	22H	M	Yes
Set Watchdog Timer	App	24H	M	Yes
Get Watchdog Timer	App	25H	M	Yes

Table 1-19. Chassis Commands (NETFUN: 00H, 01H)

Commands	NetFn	CMD	O/M	Supported
Get Chassis Capabilities	Chassis	00H	M	Yes
Get Chassis Status	Chassis	01H	M	Yes
Chassis Control	Chassis	02H	M	Yes
Chassis Reset	Chassis	03H	N	No
Chassis Identify	Chassis	04H	O	Yes
Set Front Panel Button Enables	Chassis	0AH	N	No
Set Chassis Capabilities	Chassis	05H	N	No
Set Power Restore Policy	Chassis	06H	O	Yes
Set Power Cycle Interval	Chassis	0BH	O	Yes (Default: 10 seconds)
Get System Reset Cause	Chassis	07H	N	No Restart Cause [3:0] AH = Soft reset (e.g. CTRL-ALT-DEL)
Set System Boot Options	Chassis	08H	O	Yes
Get System Boot Options	Chassis	09H	O	Yes
Get POH Counter	Chassis	0FH	M	No

Table 1-20. Event Commands (NETFUN: 04H, 05H)

Commands	NetFn	CMD	O/M	Supported
Set Event Receiver	S/E	00H	M	Yes
Get Event Receiver	S/E	01H	M	Yes
Platform Event (“Event Message”)	S/E	02H	M	Yes

Table 1-21. PEF and Alerting Commands (NETFUN: 04H, 05H)

Commands	NetFn	CMD	O/M	Supported
Get PEF Capabilities	S/E	10H	O	Yes
Arm PEF Postpone Timer	S/E	11H	O	Yes
Set PEF Configuration Parameters	S/E	12H	O	Yes
Get PEF Configuration Parameters	S/E	13H	O	Yes
Set Last Processed Event ID	S/E	14H	O	Yes
Get Last Processed Event ID	S/E	15H	O	Yes
Alert Immediate	S/E	16H	O	Yes
PET Acknowledge	S/E	17H	O	Yes

Table 1-22. SEL Commands (NETFUN: 0AH, 0BH)

Commands	NetFn	CMD	O/M	Supported
Get SEL Info	Storage	40H	M	Yes
Get SEL Allocation Info	Storage	41H	O	Yes
			Number of possible allocation units: 909 Unit size in bytes: 18 Max record size in allocation units: 18	
Reserve SEL	Storage	42H	O	Yes
Get SEL Entry	Storage	43H	M	Yes
Add SEL Entry	Storage	44H	M	Yes
Partial Add SEL Entry	Storage	45H	N	No
Delete SEL Entry	Storage	46H	O	Yes
Clear SEL	Storage	47H	M	Yes
Get SEL Time	Storage	48H	M	Yes
Set SEL Time	Storage	49H	M	Yes
Get SEL Time UTC Offset	Storage	5CH	O	Yes
Set SEL Time UTC Offset	Storage	5DH	O	Yes
Get Auxiliary Log Status	Storage	5AH	N	No
Set Auxiliary Log Status	Storage	5BH	N	No

Table 1-23. SDR Repository Commands (NETFUN: 0AH, 0BH)

Commands	NetFn	CMD	O/M	Supported
Get SDR Repository Info	Storage	20H	M	Yes
Get SDR Repository Allocation Info	Storage	21H	O Number of possible allocation units: 909 Unit size in bytes: 18 Max record size in allocation units: 18	Yes
Reserve SDR Repository	Storage	22H	M	Yes
Get SDR	Storage	23H	M	Yes
Add SDR	Storage	24H	M	Yes
Partial ADD SDR	Storage	25H	O	Yes
Delete SDR	Storage	26H	N	No
Clear SDR Repository	Storage	27H	M	Yes
Get SDR Repository Time	Storage	28H	O	Yes
Set SDR Repository Time	Storage	29H	N	No
Enter SDR Repository Update Mode	Storage	2AH	O	Yes
Exit SDR Repository Update Mode	Storage	2BH	O	Yes
Run Initialization Agent	Storage	2CH	O	Yes

Table 1-24. FRU Inventory Device Commands (NETFUN: 0AH, 0BH)

Commands	NetFn	CMD	O/M	Supported
Get FRU Inventory Area Info	Storage	10H	M FRU device ID = OOH for BMC's FRU	Yes
Read FRU Inventory Data	Storage	11H	M FRU device ID = OOH for BMC's FRU	Yes
Write FRU Inventory Data	Storage	12H	M FRU device ID = OOH for BMC's FRU	Yes

Table 1-25. Sensor Device Commands (NETFUN: 04H, 05H)

Commands	NetFn	CMD	O/M	Supported
Get Device SDR Info	S/E	20H	N	No
Get Device SDR	S/E	21H	N	No
Reserve Device SDR Repository	S/E	22H	N	No
Get Sensor Reading Factors	S/E	23H	O	Yes
Set Sensor Hysteresis	S/E	24H	O	Yes
Get Sensor Hysteresis	S/E	25H	O	Yes
Set Sensor Threshold	S/E	26H	O	Yes
Get Sensor Threshold	S/E	27H	O	Yes
Set Sensor Event Enable	S/E	28H	O	Yes
Get Sensor Event Enable	S/E	29H	O	Yes
Re-arm Sensor Events	S/E	2AH	N	No
Get Sensor Event Status	S/E	2BH	N	No
Get Sensor Reading	S/E	2DH	M	Yes
Set Sensor Type	S/E	2EH	N	No
Get Sensor Type	S/E	2FH	N	No
Set Sensor Reading and Event Status	S/E	30H	M	Yes
			Only for fan devices	

Table 1-26. Firmware Commands (NETFUN: 08H, 09H)

Commands	NetFn	CMD	Request and Response
Update Firmware	Firmware	01H	<p>REQUEST</p> <p>Byte 1 Interface Used—Interface the image is transmitted through: 00H: System interface, e.g., KCS 01H: Networking, e.g., TFTP, FTP, or HTTP 02H: USB MSC</p> <p>Byte 2 Update Type: [7]: Force update. 0H: Normal update. An update operation occurs only when the BMC validates the target board, target product, and version number. [6.0]: Reserved</p> <p>Byte 3:14 Install Options: This field is optional. If present, it contains the list of options that control the installation procedure. The number definitions are specific to the vendor.</p> <p>RESPONSE</p> <p>Byte 1 — Completion code Byte 2 — Task ID</p>

Table 1-27. Firmware Commands (NETFUN: 08H, 09H)

Commands	NetFn	CMD	Request and Response
Get Update Status	Firmware	02H	<p>REQUEST</p> <p>Byte 1 – Task ID</p> <p>RESPONSE</p> <p>Byte 1 – Completion Code</p> <p>Byte 2 – Status</p> <ul style="list-style-type: none"> • 00H: Transmitting Image • 01H: Validating Image <ul style="list-style-type: none"> • 02H: Programming • 03H: Ready to Accept Image <ul style="list-style-type: none"> • 80H: General error • 81H: Cannot establish connection • 82H: Path not found <ul style="list-style-type: none"> • 83H: Transmission Abort • 84H: Checksum error <ul style="list-style-type: none"> • 85H: Incorrect Platform • FFH: Completed <p>Byte 3 – Progression Indicator. This field is optional. If present, its value indicates the current progress of the status specified in Status byte.</p>
Copy Image Data	Firmware	03H	<p>REQUEST:</p> <p>Byte 1 – Task ID</p> <p>Byte 2 – In progress</p> <p>00H = Data transmission is in progress</p> <p>01H = Data transmission completed</p> <p>Byte 3:6 – Image offset to be copied</p> <p>Byte 7:N – Image data to be copied</p> <p>RESPONSE:</p> <p>Byte 1 – Completion Code</p>

Table 1-28. Dell OEM Commands (NETFUN: 2CH, 2DH)

Commands	NetFn	CMD	Request and Response
DCMIGetDCMICapability	OEM	01H	<p>REQUEST:</p> <p>Byte 1 – Identification</p> <p>Byte 2 – ParameterSelect</p> <p>RESPONSE:</p> <p>Byte 1 – Completion code</p> <p>Byte 2 – Identification</p> <p>Byte 3 – MajorVersion</p> <p>Byte 4 – MinorVesrion</p> <p>Byte 5 – ParameterRevision</p> <p>Byte 6~17 – ParameterData</p>
DCMIGetAssetTag	OEM	06H	<p>REQUEST:</p> <p>Byte 1 – Identification</p> <p>Byte 2 – Offset</p> <p>Byte 3 – Number</p> <p>RESPONSE:</p> <p>Byte 1 – Completion code</p> <p>Byte 2 – Identification</p> <p>Byte 3 – Length</p> <p>Byte 4~N – AssetTag Data</p>
DCMIGetDCMISensorInfo	OEM	07H	<p>REQUEST:</p> <p>Byte 1 – Identification</p> <p>Byte 2 – SensorType</p> <p>Byte 3 – EntityID</p> <p>Byte 4 – EntityInstance</p> <p>Byte 5 – Start</p> <p>Response:</p> <p>Byte 1 – Completion code</p> <p>Byte 2 – Identification</p> <p>Byte 3 – TotalNum</p> <p>Byte 4 – RecordIDNum</p> <p>Byte 5~N – SDRRecID</p>

Table 1-29. Dell OEM Commands (NETFUN: 2EH, 2FH)

Commands	NetFn	CMD	Request and Response
OemSetUbootEthaddr	OEM	21H	<p>This command is for Dedicated-NIC. After issuing the OEM command, user must reset BMC manually.</p> <p>REQUEST:</p> <p>Byte 1–17: MAC address</p> <p>Byte 18: End data – must be 00H</p> <p>RESPONSE:</p> <p>Byte 1 – Completion code</p>
OemSetUbootEth1addr	OEM	23H	<p>This command is for Shared-NIC. After issuing the OEM command, user must reset BMC manually.</p> <p>REQUEST:</p> <p>Byte 1–17: MAC address</p> <p>Byte 18: End data – must be 00H</p> <p>RESPONSE:</p> <p>Byte 1 - Completion code</p>
OemGetBMCSKU	OEM	75H	<p>REQUEST:</p> <p>REQUEST:</p> <p>Byte 1–17: MAC address</p> <p>Byte 18: End data – must be 00H</p> <p>RESPONSE:</p> <p>Byte1 – Completion code</p> <p>Byte2 – BMC SKU</p> <p>00h AST2050</p> <p>01h AST1100</p>

Table 1-30. Dell OEM Commands (NETFUN: 30H, 31H)

Commands	NetFn	CMD	Request and Response
Reserve Extended Configuration	OEM	01	<p>REQUEST:</p> <p>(None)</p> <p>RESPONSE:</p> <p>Byte 1 – Completion code</p> <p>Byte 2 – Reservation ID</p>
Get Extended Configuration	OEM	02	<p>REQUEST:</p> <p>Byte 1 – Reservation ID</p> <p>Byte 2 – Configuration ID</p> <p>Byte 3 – Attribute ID. 00H = Read entire configuration data.</p> <p>Byte 4 – Index (used by table object only)</p> <p>Byte 5 – Data Offset – LSB</p> <p>Byte 6 – Data Offset – MSB</p> <p>Byte 7 – Bytes to read. FFH = Read entire configuration or attribute</p> <p>RESPONSE:</p> <p>Byte 1 – Completion code. 01H = No more data.</p> <p>Byte 2 – Configuration ID</p> <p>Byte 3 – Attribute ID</p> <p>Byte 4 – Index (valid for table object only)</p> <p>Byte 5 – Number of bytes returned, 1-based</p> <p>Byte 6~N – Data</p>

Table 1-31. Dell OEM Commands (NETFUN: 30H, 31H)

Commands	NetFn	CMD	Request and Response
Set Extended Configuration	OEM	03	<p>REQUEST:</p> <p>Byte 1 – Reservation ID</p> <p>Byte 2 – Configuration ID</p> <p>Byte 3 – Attribute ID. 00H = Read entire configuration data</p> <p>Byte 4 - Index (used by table object only).</p> <p>Byte 5 - Data Offset – LSB</p> <p>Byte 6 - Data Offset – MSB</p> <p>Byte 7 - In progress</p> <ul style="list-style-type: none"> • [7:4] Reserved • [3:0] In progress <ul style="list-style-type: none"> • 0 – In progress • 1 – Last configuration data being transferred in this request <p>RESPONSE:</p> <p>Byte 1 – Completion code. 01H = No more data</p>
BIOSPOSTEND	OEM	80H	<p>REQUEST:</p> <p>(None)</p> <p>RESPONSE:</p> <p>Byte 1 – Completion code</p>

Table 1-32. Dell OEM Commands (NETFUN: 30H, 31H)

Commands	NetFn	CMD	Request and Response
Restore to defaults	OEM	04	<p>REQUEST:</p> <p>Byte 1 - Configuration to be restored to defaults:</p> <p>[7:5] 111b= Restore the remaining parameters not included in below lists. 000b= Remaining parameters stay what it is. All other values are reserved</p> <p>[4] 1b= Restore PEFs to defaults [3] 1b= Restore serial configuration parameters to defaults [2] 1b= Restore SOL configuration parameters to defaults [1] 1b= Restore LAN configuration parameters to defaults [0] 1b= Restore user accounts to defaults</p> <p>RESPONSE:</p> <p>Byte 1 - Completion Code CCh = restore to one or more of the configuration not supported. Byte 2 - Task ID.</p> <p>Use the Task ID to get the restore status. The Task ID is automatically become invalid after 120 seconds when the restore requesting is completed. 00h reserved.</p>
Get Restore Status	OEM	05	<p>REQUEST:</p> <p>Byte 1 - Task ID Task ID, the value returned by previous call to Restore to Defaults command.</p> <p>RESPONSE:</p> <p>Byte 1 - Completion Code Byte 2 - Default Restore Status: 00h: Restore in progress 01h: Restore completed</p>

Table 1-33. Dell OEM Commands (NETFUN: 30H, 31H)

Commands	NetFn	CMD	Request and Response
SETSYSTEMGUID	OEM	B3H	REQUEST: Byte 1 ~16 – System GUID RESPONSE: Byte 1 – Completion code

Table 1-34. Vendor OEM Commands (NETFUN: 34H, 35H)

Commands	NetFn	CMD	Request and Response
Set Asset Tag	OEM	12H	REQUEST: Byte 1 – Length Byte 2~11 – Data (Max Set Asset Tag Length – 0x0A) RESPONSE: Byte 1 – Completion code Byte 2 – Count written

Table 1-35. Vendor OEM Commands (NETFUN: 34H, 35H)

Commands	NetFn	CMD	Request and Response
Set LAN Source	OEM	13H	REQUEST: Byte 1 – LAN Source <ul style="list-style-type: none"> • 00H – Shared NIC • 01H – Dedicated NIC RESPONSE: Byte 1 – Completion code Byte 2 – LAN source setting
Get LAN Source	OEM	14H	REQUEST: (None) RESPONSE: Byte 1 – Completion code Byte 2 – Current LAN source <ul style="list-style-type: none"> • 00H – Shared NIC • 01H – Dedicated NIC
GetFCBFWVersion	OEM	16H	REQUEST: (None) RESPONSE: Byte 1 – Completion code Byte 2 – FCB F/W Major Version Byte 3 – FCB F/W Minor Version

Table 1-36. Vendor OEM Commands (NETFUN: 34H, 35H)

Commands	NetFn	CMD	Request and Response
SetFanControl	OEM	61H	<p>REQUEST:</p> <p>Byte 1 – Fan Control Setting</p> <p>[7] - Enabled/Disabled FAN Control</p> <p>0: Disabled(Default)</p> <p>1: Enabled</p> <p>[6:0] - Duty Cycle Setting. The range is from 0 to 100, others are reserved.</p> <p>RESPONSE:</p> <p>Byte 1 – Completion code</p>
GetFanControl	OEM	62H	<p>REQUEST:</p> <p>(None)</p> <p>RESPONSE:</p> <p>Byte 1 – Completion code</p> <p>Byte 2 – Fan Control Setting</p> <p>[7] - Enabled/Disabled FAN Control</p> <p>0: Disabled(Default)</p> <p>1: Enabled</p> <p>[6:0] - Duty Cycle Setting. The range is from 0 to 100, others are reserved.</p>

Table 1-37. Vendor OEM Commands (NETFUN: 34H, 35H)

Commands	NetFn	CMD	Request and Response
SetFSCTable	OEM	63H	<p>REQUEST:</p> <p>Byte 1 – FSC Table Setting [7] – Enabled/Disabled FAN Table 0h: Disabled (Default) 1h: Enabled [6:0] – Fan Table Setting(o-based) 80h: 1st FSC fan table (default: 13800RPM) 81h: 2nd FSC fan table (FACEBOOK) 82h: 3rd FSC fan table (Oscillation) 83h: 4th FSC fan table (Western Geco) 84h: 5th FSC fan table (Loki) Byte 2 – FSC Table Privilege Default: 0x00 Bit 0: Set by BIOS Bit1: Set by User (Higher bit has higher privilege.) P.S. Exception action of privilege – Back to default Byte1: 0x00 Byte2: 0x00</p> <p>RESPONSE:</p> <p>Byte 1 – Completion code</p>
GetFSCTable	OEM	64H	<p>REQUEST:</p> <p>(None)</p> <p>RESPONSE:</p> <p>Byte 1 – Completion code Byte 2 – FSC Table Setting [7] – Enabled/Disabled FAN Table 0h: Disabled (Default) 1h: Enabled [6:0] – Fan Table Setting(o-based) 80h: 1st FSC fan table (default: 138RPM) 81h: 2nd FSC fan table (FACEBOOK) 82h: 3rd FSC fan table (Oscillation) 83h: 4th FSC fan table (Western Geco) 84h: 5th FSC fan table (Loki) Byte 3 – FSC Table Privilege Default: 0x00 Bit 0: Set by BIOS Bit1: Set by User (Higher bit has higher privilege.)</p>

Chassis Control Command Implementation

Table 1-38. Chassis Control Command (NetFn=00/01,

Cmd=02h) Request Data Byte 1-Bit [3:0]	Description
0h=Power Down off.	BMC issues a signal to simulate the ACPI-compliant 4 second power off.
01=Power On	Power on.
2h=Power Cycle	Power cycle.
3h=Hard Reset	Hard reset.
4h=Pulse Diagnostic Interrupt	BMC issues a NMI signal to the system.
5h=Soft Shutdown	BMC triggers a power button signal.

Entity ID and Instance Table

Table 1-39. Entity ID and Instance Table

Entity ID	Entity Instance	Entity Name	Sensor Numbers
	01h	VCORE1	51h
	02h	VCORE2	52h
03h (Processor)	03h	CPU1Status	41h
	04h	CPU2Status	42h
06 (System Management Module)	00h	Security	75h
	00h	SEL Fullness	40h
	01h	Memory	60h
	02h	PS 12V	14h
	03h	PS 5V	15h
	04h	STBY 3.3V	16h
07h (System Board)	05h	PEF Action	71h
	06h	WatchDog2	72h
	07h	ACPI Pwr State	73h
	08h	AC Pwr On	74h
	09h	1 AC Status	A8h
	0Ah	2 AC Status	A9h
	0Bh	PCi BUS	A5h
	01h	FCB FAN 1	01h
	02h	FCB FAN 2	02h
1Dh (Fan/Cooling Device)	03h	FCB FAN 3	03h
	04h	FCB FAN 4	04h
	01h	FCB Ambient 1	2Ah
40h (Inlet Temperature)	02h	FCB Ambient 2	2Bh
	01h	Processor 1 Temp	61h
41h (CPU Temperature)	02h	Processor 2 Temp	62h
	01h	MLB TEMP 1	21h
42h (Baseboard Temperature)	02h	MLB TEMP 2	22h
	03h	MLB TEMP 3	23h

Table 1-40. Entity ID and Instance Table

Entity ID	Entity Instance	Entity Name	Sensor Numbers
0Ah (Power Supply)	01h	PS Current	A1h
	02h	PSU 1 POUT	A3h
	03h	PSU 2 POUT	A4h
	08h	PSU 1 Present	A6h
	09h	PSU 2 Present	A7h

Sensor Summary

In the Offset column:

AM = Assertion

mask

DM = Deassertion mask

RM = Reading mask

SC = Sensor capabilities

SI = Sensor initialization

TM = Settable/Readable threshold mask

Table 1-41. Sensor Summary

Sensor Number	Sensor Name	Sensor Type	Event/Reading Type	Offset
21h	MLB TEMP1	Temperature (01h)	Threshold (01h)	SI: 7Fh
22h	MLB TEMP 2			SC: E8h
23h	MLB TEMP 3			AM: 0A80h DM: 7A80h TM: 3838h
61h	Processor 1 Temp	Temperature (01h)	Threshold (01h)	SI: 7Fh SC:
62h	Processor 2 Temp			E8h AM: 0A80h DM: 7A80h TM: 3838h
2Ah	FCB Ambient1	Temperature (01h)	Threshold (01h)	SI: FCh SC:
2Bh	FCB Ambient2			E8h AM: 0200h DM: 2000h TM: 3030h

Table 1-42. Sensor Summary

Sensor Number	Sensor Name	Sensor Type	Event/Reading Type	Offset
14h	PS 12V	Voltage (02h)	Threshold (01h)	SI: 7Bh
15h	PS 5V			SC: E8h
16h	STBY 3.3V			AM: 7A95h DM: 7A95h TM: 3F3Fh
51h	VCORE 1	Voltage (02h)	Threshold (01h)	SI: 7Fh SC:
52h	VCORE 2			E0h AM: 0000h DM: 0000h TM: 3838h
01h	FCB FAN1	Fan (04h)	Threshold (01h)	SI:FCh
02h	FCB FAN2			SC: E8h
03h	FCB FAN3			AM: 2004h
04h	FCB FAN4			DM: 0000h TM: 3A3Ah
41h	CPU1Status	Processor (07h)	Sensor-specific (6Fh)	SI:63h
42h	CPU2Status			SC:C0h AM:0012h DM:0000 h TM:0012h
40h	SEL Fullness	Event Logging Disable (10h)	Sensor-specific	SI: 63h SC: 40h AM: 0034h DM: RM: 0034h
60h	Memory	Memory (0Ch)	Sensor-specific (6Fh)	SI: 63h SC: 40h AM: 0023h DM: RM: 0023h

Table 1-43. Sensor Summary

Sensor Number	Sensor Name	Sensor Type	Event/Reading Type	Offset
71h	PEF Action	System Event (12h)	Sensor-specific (6Fh)	SI: 63h SC: 40h AM: 0010h DM: 0000h RM: 0010h
72h	WatchDog2	WatchDog2 (23h)	Sensor-specific (6Fh)	SI:63h SC:40h AM:010Fh DM:0000 RM:010Fh
73h State	ACPI Pwr State	System ACPI Power (22h)	Sensor-specific (6Fh)	SI: 63h SC:40h AM: 1800h DM: 0000hRM: 1800h
74h	AC Pwr On	Power Unit (09h)	Sensor-specific (6Fh)	SI: 63h SC: 40h AM: DM: 0010h RM: 0010h
75h Violation	Security	Platform Security Attempt (06h)	Sensor-specific (6Fh)	SI: 63h SC: 40h AM: 0020h DM: 0000h RM: 0020h
A1h	PS Current	Current (03h)	Threshold (01h)	SI: D1h SC: Coh AM: DM: TM: 3838h

Table 1-44. Sensor Summary

Sensor Number	Sensor Name	Sensor Type	Event/Reading Type	Offset
A3h	PSU 1 POUT	Current (03h)	Threshold (01h)	SI: Coh
A4h	PSU 2 POUT			SC: Coh AM: 0000h DM: 0000h TM: 0000h
A5h	PCI BUS	Critical Interrupt (13h)	Sensor-specific (6Fh)	SI: 63h SC: 40h AM: 0030h DM: 0000h RM: 0030h
A6h	PSU 1 Present	Power Supply (08h)	Sensor-specific (6Fh)	SI: 60h
A7h	PSU 2 Present			SC: 40h AM: 0040h DM: 0001h RM: 0003h
A8h	PSU 1 AC Status	Power Unit (09h)	Sensor-specific (6Fh)	SI: 60h
A9h	PSU 2 AC Status			SC: 40h AM: 0010h DM: 0010h RM: 0011h
18h	NM Exception	DCh	72h	
19h	NM Health	DCh	73h	
1Ah	NM Capabilities	DCh	74h	
1Bh	NM Threshold	DCh	72h	
Coh	No sensor name (NM Discovery)	00h	00h	

Threshold Settings and Converting Formulas

Table 1-45. Threshold Settings and Converting Formulas

Sensor Number	Sensor Name	The Converting Formula					
		Upper non-recoverable	Upper critical	Upper non-critical	Lower non-recoverable	Lower critical	Lower non-critical
Fan							
01h	FCB FAN1	Actual_Reading (RPM) = Raw_Data x 100					
		0xFF	0xFF	0xFF	0x00	0x0F	0x00
02h	FCB FAN2	Actual_Reading (RPM) = Raw_Data x 100					
		0xFF	0xFF	0xFF	0x00	0x0F	0x00
03h	FCB FAN3	Actual_Reading (RPM) = Raw_Data x 100					
		0xFF	0xFF	0xFF	0x00	0x0F	0x00
04h	FCB FAN4	Actual_Reading (RPM) = Raw_Data x 100					
		0xFF	0xFF	0xFF	0x00	0x0F	0x00
Voltage							
14h	PS 12V	Actual_Reading (Volts) = Raw_Data x 0.062					
		0xD8	0xD4	0xCF	0xAB	0xAF	0xB4
15h	PS 5V	Actual_Reading (Volts) = Raw_Data x 0.026					
		0xD7	0xD3	0xCD	0xA9	0xAE	0xB3
16h	STBY 3.3V	Actual_Reading (Volts) = Raw_Data x 0.0172					
		0xD6	0xD3	0xCD	0xA9	0xAD	0xB3
51h	VCORE 1	Actual_Reading (Volts) = Raw_Data x 0.0083					
		0xFF	0xFF	0xFF	0x00	0x00	0x00

Table 1-46. Threshold Settings and Converting Formulas

Sensor Number	Sensor Name	The Converting Formula					
		Upper non-recoverable	Upper critical	Upper non-critical	Lower non-recoverable	Lower critical	Lower non-critical
52h	VCORE 2	Actual_Reading (Volts) = Raw_Data x 0.0116					
		0xFF	0xFF	0xFF	0x00	0x00	0x00
Temperature							
21h	MLB TEMP 1	Actual_Reading (degrees C) = Raw_Data					
		0x5A	0x57	0x55	0x00	0x00	0x00
22h	MLB TEMP 2	Actual_Reading (degrees C) = Raw_Data					
		0x5A	0x57	0x55	0x00	0x00	0x00
23h	MLB TEMP 3	Actual_Reading (degrees C) = Raw_Data					
		0x5A	0x57	0x55	0x00	0x00	0x00
61h	Processor 1 Temp	Actual_Reading (degrees C) = Raw_Data					
		0x5A	0x55	0x51	0x00	0x00	0x00
62h	Processor Temp 2	Actual_Reading (degrees C) = Raw_Data					
		0x5A	0x55	0x51	0x00	0x00	0x00
2Ah	FCB Ambient1	Actual_Reading (degrees C) = Raw_Data					
		0xFF	0x32	0x00	0x00	0x00	0x00
2Bh	FCB Ambient2	Actual_Reading (degrees C) = Raw_Data					
		0xFF	0x32	0x00	0x00	0x00	0x00

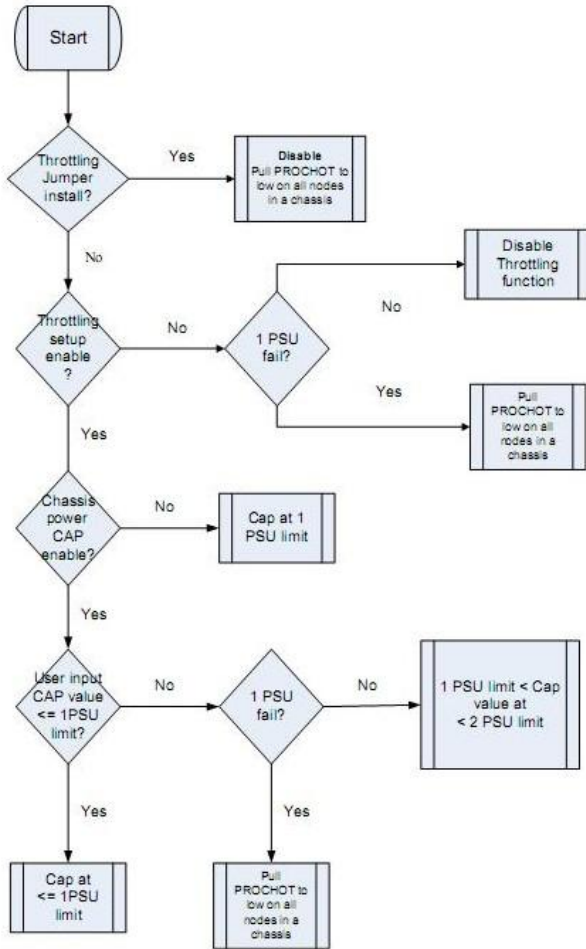
Table 1-47. Threshold Settings and Converting Formulas

Sensor Number	Sensor Name	The Converting Formula					
		Upper non-recoverable	Upper critical	Upper non-critical	Lower non-recoverable	Lower critical	Lower non-critical
Power Supply							
A1h	PS Current	Actual_Reading = Raw_Data					
		0xFF	0xFF	0xFF	0x00	0x00	0x00
		Upper non-recoverable	Upper critical	Upper non-critical	Lower non-recoverable	Lower critical	Lower non-critical
A3	PSU 1 POUT	Actual_Reading = Raw_Data					
		0xFF	0xFF	0xFF	0x00	0x00	0x00
A4	PSU 2 POUT	Actual_Reading = Raw_Data					
		0xFF	0xFF	0xFF	0x00	0x00	0x00

Power Throttling Function

Power Throttling Function Flow Chart

V1.8



Power Throttling Configuration in BIOS Setup Utility

Before enabling the power throttling feature, you must set the Power Management option to Active Power Controller or Node Management. Access this option through the BIOS setup utility's Server menu. Then from the Server menu you can enable or disable power throttling and power CAP, and set the chassis CAP value.

Only MB4 can display the power throttling behavior setting in the BIOS setup menu.

Additional Power Throttling Information

- The power throttling feature takes advantage of the node management function to control CPU frequency.
- If the chassis CAP function is disabled and power throttling is enabled, the BMC will set a power supply unit (PSU) limit of one as the chassis CAP value.
- After the power throttling and chassis CAP settings are changed, the main logic board (MLB) must be restarted.
- The power cap feature cannot be enabled concurrently with the Intel® Data Center Manager (DCM).

Power Throttling Protection

The power throttling feature is a full power redundancy feature. This feature adjusts CPU frequency via a PROCHOT# signal to reduce the MLB's power consumption.

Information From the Fan Control Board

BMC can get the following information from the fan control board:

- FW version
- Board ID
- Ambient1 Reading
- Ambient2 Reading
- Fan Tach1 Reading
- Fan Tach2 Reading
- Fan Tach3 Reading
- Fan Tach4 Reading
- PSU Current Reading

Extended Configurations

Table 1-48. Configuration ID = 02h, NIC

Attribute	ID	Size	Description
NicSelection	1	1	Specifies the current mode of operation for the BMC network interface. o: Shared NIC (default) i: Dedicated NIC

Table 1-49. Configuration ID = 03h, SOL

Attribute	ID	Size	Description
SOL Idle Timeout	1	2	byte1:2 - Define the inactivity timeout in minutes, 1-based, LSByte first. This parameter only applies to the IPMI over LAN session with SOL payload activated. oh= session does not timeout and close due to inactivity. Default = 01h
Telnet/SSH Redirect Enable	2	1	0: Disabled (default) 1: Enabled

Table 1-50. Configuration ID = 04h, Security

Attribute	ID	Size	Description
Service Disabled	1	1	Disable or enable services. This attribute takes precedence over the individual feature enabled/disabled. Once one service has been disabled, the BMC must not allow user to enable the corresponding feature and D5h completion code must be returned. For example, if HTTP/HTTPS is disabled, user must not allow to enable the Web Server through Web Server Configuration (Configuration ID 0Ch). In other words, Web can only be disabled or enabled when HTTP/HTTPS is enabled. [0] - all service except IPMI are disabled. This bit takes precedence over other bits. Default is 0. [1] - KVM/Virtual Storage, enabled by default. [2] - HTTP/HTTPS, enabled by default. [3] - SSH/Telnet, disabled by default.
Max Authentication Failures	2	1	Specifies the maximum number of allowed authentication failures. Setting this value to 0 will disable the lockout feature. When an account is lockout, the IPMI Messaging must be disabled on the LAN channel. See Get User Access command. Default = 00h (disable Lockout feature)

Lockout Window	3	2	Specifies the window, in second, during which if the consecutive maximum number of authentication failures is reached, the account should be disabled. Setting this value to 0 will disable the lockout feature. Default setting is 180 seconds.
Lockout Time	4	2	Specifies the time period an account should be disabled if the maximum number of authentication failures is reached. The unit is second. Setting this value to 0 will disable the lockout feature. Default value is 3600 (1 hour).

Table 1-51. Configuration ID = 06h, DNS

Attribute	ID	Size	Description
DNS Dhcp Enable	1	1	Specifies that the DNS server IP addresses should be assigned from the DHCP server. 0: FALSE (default) 1: TRUE.
DNS Server1	2	4	Specifies the IP address for DNS server 1. This parameter is read-only if DNS Dhcp Enable and DHCP are enabled.
DNS Server2	3	4	Specifies the IP address for DNS server 2. This parameter is read-only if DNS Dhcp Enable and DHCP are enabled.
DNS Register BMC	4	1	Enable registering the BMC host name on the DNS server 0: FALSE (default) 1: TRUE.
DNS BMC Host Name	5	1..64	Specifies the DNS BMC host name. This parameter is read-only if DNS Register BMC is set to TRUE. At least one character must be alphabetic. The default name is bmc-service_tag, where service_tag is the service tag number of the Dell server. For example: bmc-XG3487A.
DNS Domain Name Dhcp Enable	6	1	Specifies that the DNS domain name should be assigned from the DHCP server. 0: FALSE (default) 1: TRUE.
DNS Domain Name	7	1..256	The DNS domain name string. This parameter is read-only if DNS Domain Name Dhcp Enable is set to TRUE. Characters are restricted to alphanumeric, '-' and '.'. Default is ""

Table 1-52. Configuration ID = 0Ch, WEB Server Configuration

Attribute	ID	Size	Description
Web Server Enabled	1	1	Disable or enable the BMC Web server. 0: FALSE 1: TRUE (default)
Max Web Sessions	2	1	The maximum number of simultaneous sessions allowed for this system. This field is READ-ONLY.
Active Web Sessions	3	1	The number of current session for GUI on the system. This field is READ-ONLY.
Web Server Timeout	4	4	The WEB communication idle timeout, in seconds. Timeout range is 60 to 1920 seconds. A 0 specifies disabling the timeout feature. The default is 300
HTTP Port Num	5	2	Specifies the port number to use for HTTP communication with the BMC. Default is 80.
HTTPS Port Num	6	2	Specifies the port number to use for HTTPS communication with the BMC. Default is 443.

Table 1-53. Configuration ID = 0Eh, Firmware Log, indexed object

Attribute	ID	Size	Description
Entity	1	1	Refer to Firmware Information configuration.
Firmware Version	2	1..16	Refer to Firmware Information configuration.
Branch	3	1..16	Refer to Firmware Information configuration.
Build Information	4	1..16	Refer to Firmware Information configuration.
Update Date / Time	5	3	Number of minutes from 0:00 hrs 1/1/08. LSbyte first (little endian).

Table 1-54. Configuration ID = 0Fh, Firmware Information, indexed object

Attribute	ID	Size	Description
Name	1	1..16	Specifies BMC model name, such as AST2050.
Description	2	1..256	A text description of the type controller.

Entity	3	1	Specifies the entity of the controller. 0: BMC 1: SYSTEM (BIOS) 2: PDB 3: FCB.
Product Info	4	1..64	Refer to Firmware Information configuration.
Firmware Version	5	1..16	Number of minutes from 0:00 hrs 1/1/08. LSbyte first (little endian).
Branch	6	1..16	A string containing the firmware branch information.
Build Information	7	1..16	A string containing the firmware build number information. The string format is YYMMDD.

Table 1-55. Configuration ID = 10h, Firmware Update

Attribute	ID	Size	Description
Remote Update Enable	1	1	Allow firmware update via TFTP server.
Protocol	2	1	Specified supported protocols. [7:3] - reserved [2] - HTTP [1] - FTP [0] - TFTP.
URI	3	1..256	The URI of the image file.
Connection Retry	4	1	Specify the number of retries for connecting to TFTP server. A zero value means the BMC does not attempt to retry connect to TFTP server.
Retry Interval	5	1	Define the retry interval in 5 seconds increments.
Delay Time	6	1	Define the delay time for start connecting to TFTP server. The time is specified in second. 00h: The BMC start connecting to TFTP server immediately. FFh: random between 5 and 10 seconds.

Table 1-56. Configuration ID = 11h, Power Management

Attribute	ID	Size	Description
Power Management Enable	1	1	Specify the use of power management method. Bit 7: Enable DPNM power management 1b = enable DPNM 0b = disable DPNM Bit 6:0: reserved
Power Staggering AC Recovery	2	1	This parameter is only effective if the Power Policy is not set to always off. 0x00 : Immediate PowerOn (No Delay) : Default 0x01 : Auto (Random), the auto generated delay time must be in the range of Minimum Power On Delay and Maximum Power On Delay. 0x02 : User Defined, the user defined delay time must be in the range of Minimum Power On Delay and Maximum Power On Delay.
Power On Delay	3	2	Define the time to delay power on the system after AC recovered.
Minimum Power On Delay	4	2	Specify the minimum power on delay time when AC is restored. This should not be less than the time BMC startup time.
Maximum Power On Delay	5	2	Specify the maximum power on delay time when AC is restored. The number must large than Minimum Power On Delay.

Appendix

SSH/Telnet Enable and Disable

- Reserved extended configuration (NetFn: 30H CMD:01H)
- Set/Get extended configuration (NetFn: 30H CMD:03H/02H)

Table 1-57. Configuration ID = 04h, Security

Attribute	ID	Size	Description
Service Disabled	1	1	<p>Disable or enable services. This attribute takes precedence over the individual enabled/disabled feature. Once a service has been disabled, the BMC must not allow the user to enable the corresponding feature, and the D5h completion code must be returned.</p> <p>For example, if HTTP/HTTPS is disabled, the user is not allowed to enable the web server through the web server configuration (configuration ID 0Ch). In other words, the web server can only be disabled or enabled when HTTP/HTTPS is enabled.</p> <p>[0] – All service except IPMI is disabled. This bit takes precedence over other bits. Default is 0.</p> <p>[1] – KVM/Virtual Storage, enabled by default.</p> <p>[2] – HTTP/HTTPS, enabled by default.</p> <p>[3] – SSH/Telnet, disabled by default.</p>

Examples:

Get SSH/Telnet enable status:

- Reserved extended configuration:
`ipmitool 0x30 0x01`
Response: 0x01 (Reservation ID)
- Get extended configuration:
`ipmitool 0x30 0x02 0x01 0x04 0x01 0x00 0x00 0x00 0xFF`
Response: 0x04 0x01 0x00 0x01 0x08 (SSH/Telnet disabled)

Set SSH/Telnet enable:

- **Reserved extended configuration:**
ipmitool 0x30 0x01
Response: 0x02 (Reservation ID)
- **Enable SSH/Telnet:**
ipmitool 0x30 0x03 0x02 0x04 0x01 0x00 0x00 0x00 0x01 0x00 (set [3] SSH/Telnet to o)
Response: 0x01

SSH/Telnet Enable and Disable

- Reserved extended configuration (NetFn: 30H CMD:01H)
- Set/Get extended configuration (NetFn: 30H CMD:03H/02H)

Table 1-58. Configuration ID = 03h, SOL

Attribute	ID	Size	Description
Telnet/SSH	2	1	[0] – Disabled (default)
Redirect Enable			[1] – Enabled

Examples:**Get SSH/Telnet redirect enable status:**

- **Reserved extended configuration:**
ipmitool 0x30 0x01
Response: 0x01 (Reservation ID)
- **Get extended configuration:**
ipmitool 0x30 0x02 0x01 0x03 0x02 0x00 0x00 0x00 0xFF
Response: 0x03 0x02 0x00 0x01 0x00 (SSH/Telnet SOL redirect disabled)

Set SSH/Telnet SOL redirect enable:

- **Reserved extended configuration:**
ipmitool 0x30 0x01
Response: 0x02 (Reservation ID)
- **Enable SSH/Telnet SOL redirect:**
ipmitool 0x30 0x03 0x02 0x03 0x02 0x00 0x00 0x00 0x01 0x01 (set 1 to enable)
Response: 0x01

VLAN ID

Use the LAN configuration command parameter 14H to set or get the VLAN ID. For additional information, refer to the IPMI v2.0 specifications.

Table 1-59. VLAN Commands

Commands	NetFn	CMD	O/M	Supported
Set LAN Configuration Parameters (Parameter 9 and 25 are not supported)	Transport	01h	M	Yes
Get LAN Configuration Parameters (Parameter 9 and 25 are not supported)	Transport	02h	M	Yes

Table 1-60. LAN Configuration Parameter 14H

Parameter	#	Parameter Data
802.1q VLAN ID (12-bit)	14H	<p>Data 1</p> <p>[7:0] – Least significant 8-bits of the VLAN ID. 00h if VLAN ID not used.</p> <p>Data 2</p> <p>[7] – VLAN ID enable.</p> <p>0b – Disabled 1b – Enabled</p> <p>If enabled, the BMC will only accept packets for this channel if they have 802.1q fields and their VLAN ID matches the VLAN ID value given in this parameter.</p> <p>[6:4] – Reserved</p> <p>[3:0] – Most significant 4-bits of the VLAN ID</p>

Examples:

Set VLAN ID:

- Get LAN configuration parameter:

```
ipmitool 0xC0 0x02 0x01 0x14 0x00 0x00
```

Response: 0x00 0x11 0x01 0x80 (VLAN Enable and VLAN ID: 1)
- Set LAN configuration parameter:

```
ipmitool 0xC0 0x01 0x01 0x14 0x01 0x80
```

Response: 0x00

BMC/BIOS Version Information

The Get Device command is used to retrieve the intelligent device's hardware revision, firmware/software revision, and sensor and event interface command specification revision information. For additional information, refer to the IPMI v2.0 specifications.

Table 1-61. Get Device Command

Response Data	Data Field
Byte 1	Completion code
Byte 2	Device ID
Byte 3	Device revision [7] 1 – Device provides device SDRs 0 – Device does not provide device SDRs [6:4] – Reserved. Return as 0. [3:0] – Device Revision, binary encoded
Byte 4	Firmware revision 1 [7] – Device available 0 = Normal operation 1 = Device firmware, SDR repository update or self-initialization in progress. Firmware/SDR repository updates can be differentiated by issuing a Get SDR command and checking the completion code. [6:0] – Major firmware revision, binary encoded
Byte 5	Firmware revision 2: Minor firmware revision. BCD encoded

Example:

Get device ID:

```
ipmitool mc info
```

```
Response: 0x00 0x25 0x01 0x01 0x00 0x02 0xbf 0xa9 0x19 0x00 0x3b 0x00  
0x6e 0x6d 0x00 0x00
```

This indicates that the BMC version is V1.00.

BIOS Version Information

The BIOS enables the system interface to the BMC and logs this event to the BMC early in POST. BIOS version information is located in the event record, bytes 15 and 16.

Table 1-62. POST Start Event

Byte	Item	Data
1-2	Record ID	
3	Record Type	
4-7	Timestamp	
8-9	Generator ID	0x01 (BIOS)
10	Event Message Format Version	0x04 (IPMI 1.5)
11	Sensor Type	0xC1 (OEM reserved)
12	Sensor Number	0x81 (BIOS start)
13	Event Direction/Event Type	0x70 (OEM)
14	Event Data 1	0xA0
15	Event Data 2	0x01 (BIOS major version)
16	Event Data 3	0x01 (BIOS minor version)

Example:

SEL list command:

```
ipmitool sel get 9
```

This indicates that the BIOS version is V1.1.

```
SEL Record ID      : 0009
Record Type       : 02
Timestamp        : 01/13/2011 21:26:28
Generator ID     : 0001
EvM Revision     : 04
Sensor Type      : Unknown
Sensor Number    : 81
Event Type       : OEM
Event Direction  : Assertion Event
Event Data       : a00101
Description      :
```