hp integrity rx2600 and hp integrity rx5670 Management Processor Card Firmware Upgrade Product Update

Manufacturing Part Number: rx2600rx56xx_update
September 2003

U.S.A.

Warranty and Support

Refer to the warranty statement provided with your original HP Server system documentation for the warranty limitations, customer responsibilities, and other terms and conditions.

HP Repair and Telephone Support

Refer to the *Warranty & Support for your HP Server* booklet supplied with your HP Server system documentation for instructions on how to obtain HP repair and telephone support.

Related Documents

The latest version of this document, and any updates, are posted under the appropriate server at http://docs.hp.com and www.hp.com/support/itaniumservers.

1 Management Processor Card Firmware

Introduction

This document is intended to provide information on the supported operating environment for the management processor (MP) and to provide installation instructions for upgrading the MP processor card firmware to the latest release:

- MP features
- Supported browsers
- Additional commands available for the MP processor card firmware

Management Processor Card Firmware Features

The MP processor card features may be mirrored or not mirrored. Any combination of mirroring and private commands may be executed at one time. Only a mirroring console is affected by the results of actions taken by other members of the same mirroring set. The following console modes are available:

- System console redirection
- Console mirroring

System Console Redirection

The system console redirection mode allows the system's console to be redirected to any of several remote console clients connected to the MP without the system being aware of where the console I/O is being directed. The console clients may interact with the system as if they were all sitting in front of the local console. Only one of the consoles can write at a time. This functionality is available for the system's firmware and operating system.

Graphic redirection is not intrinsically part of MP functionality, but the MP architecture supports, to some extent, the transport of raw data and in particular graphic redirection with the assistance of some additional software (SharedX for HP-UX, display redirection, and so on).

Console Mirroring

Console mirroring provides the ability to mirror the system console display across several console clients and share their keyboards while several console users simultaneously access the system's console. The following consoles may be mirrored:

- Local serial console
- Remote console
- LAN console

- WEB console

The display mirroring is implemented by sending, for each console client connected to the MP CO command, the same console output data flow. Keyboard sharing is implemented by merging all inputs coming from each console client connected to the MP. The MP allows only one user to have write access to the shared console at a time. If a mirrored console user attempts to type on the console and does not have write access, the user is notified by an informative message:

```
[Read only - use ^Ecf for console write access.]
```

To gain write access to the system console, enter:

<^ (control)ecf> keys

That is, while holding down the **Control key**, press the **e** key, then release the **Control key** and press the **c** and **f** keys. Write access is retained until another user requests console write access.

Mirroring is implemented consistently with the access control rules that use a user logon and password. However once a client has gained access to the MP, the user is able to access the redirected system's console without any restrictions. The only restrictions are that only one console user may type at a time and that console write access has to be granted.

MP Command Mode

The MP Command Mode is available through a user interface from any console client connected to the MP. This is an interactive process that may be activated by the console client from the Main Menu. The following features are available from MP Command Mode:

- Status and control of Locator LED
- Access to BMC data: FRU information, system power state, temperature information, power supplies, and fan status
- Control of system power, resets, and Transfer of Control (TOC) via IPMI commands to BMC
- Local serial port configuration: speed, flow control, other serial parameters
- Remote serial port configuration: modem to use, speed, modem protocol (Bell, CCITT)
- Access Control configuration: MP user login accounts, dial-back number for remote modem port, user capabilities (Administrator/Operator)
- Flow Control timer configuration (maximum XOFF delay)
- Login process timers
- Session inactivity timer configuration
- Enable/Disable remote, telnet, web console access
- Diagnostics: modem selftest, I^2C connection, LAN access (PING), MP parameters checksum
- MP Command Mode inactivity timeout configuration
- MP reset
- MP firmware upgrade

Management Processor Card Firmware Browser Support

The following browsers are supported by the Management Processor Card firmware:

Browser	Version	Operating System						
		HP-UX		Windows				LINUX
		11i	11	2000	98	95	NT	2.2
MONZILLA	0.9.9							X
INTERNET EXPLORER	6.0			X	X		X	
	5.5			X	X	X	X	
	5.01			X	X	X	X	
NETSCAPE	6.2.3			X	X	X	X	X
	6.2.1 (Requires GTK and 1.2.10 Support Library)	X	X					

Additional MP Menu Based Commands

The following additional commands are now available:

- CE: Log Repair Information
- FP: Front Panel Processes
- MA: Return to Main Menu
- XU: MP Firmware Update (FW alias)

CE: LOG REPAIR INFO IN HISTORY BUFFER

The CE command allows the operator to save the result of a repair or firmware change in the history buffer. There are no parameters for the command. Examples for executing the command using the Menu-Based and Command Line interfaces follow.

Menu-Based Command Interface

The menu-based command interface allows repair and firmware update messages to be logged from the same input screen. A sample session follows.

```
MP  Host Name: hqmaess1
MP:CM>  CE

Type of Operation Menu:

     F - Firmware update
     R - Repair

Enter menu item or [Q] to Quit: R

Enter message to be logged (32 characters max): CPU was replaced

-> Message has been logged

MP Host Name: hqmaess1
MP:CM>
```

Command Line Interface

The commands to record repair, firmware, or text messages on a command line are:

- Repair
- Firmware
- Text message

Repair Command Message

```
P:CM> ce -repair This is the message to be logged
```

Firmware Command Message

```
MP:CM> ce -firmware This is the message to be log
```

Text Message

```
MP:CM> ce -r This is a text message to be logged
```

FP: FRONT PANEL PROCESS

This command allows the modification of the state of the front panel. Specifically, it provides the ability to turn off the Fault and Attention LEDs, as well as turn on/off the Locator LED.

Menu-Based Command

To modify the front panel using the menu-based commands, complete the following procedure:

```
MP Host Name: hqiasle8

MP:CM> FP

This command allows a user modify the state of the front panel.

LEDs:    SYSTEM        POWER
FLASH YELLOW  ON
LED State: Running non-OS code.  Non-critical error detected.
Check Events and Console Logs for error messages.
Current Front Panel State:

  - - Fault Condition : Off
W - Attention Condition : On
L - Locator LED         : Off

Enter parameter(s) to change, A to modify All, or [Q] to Quit: A

For each parameter, enter:
New value, or <CR> to retain the current value, or
DEFAULT to set the default value, or
Q to quit

Attention Condition:
Current -> - - - On
OFF - Off

Enter new value, or [Q] to Quit: OFF
-> Attention Condition will be updated.

Locator LED State:
ON  - On
Current -> OFF - Off

Enter new value, or [Q] to Quit: ON

-> Locator LED State will be updated.

New Front Panel State (* modified values):
- - Fault Condition     : Off
* W - Attention Condition : Off
* L - Locator LED         : On

Enter parameter(s) to change, Y to confirm changes, or [Q] to Quit: Y

-> Front Panel State has been updated.

LEDs:    SYSTEM        POWER
```

```
         FLASH GREEN   ON

LED State: Running non-OS code.
MP Host Name: hqiasle8
MP:CM>
```

Command Line Interface

The following table lists the LED commands available from the command line interface:

Condition	Command	Result
Turn off Fault	`fp -f off`	Fault conditions are no longer reported.
Turn off Attention	`fp -w off`	Warning messages are no longer displayed
Turn on Locator LED	`fp -l`	Locator LED is active

Display current settings from the command line	`fp -nc`	`LEDs:  SYSTEM  POWER`
		`FLASH GREEN  ON`
		
		`LED State: Running non-OS code.`
		
		`Current Front Panel State:`
		`Fault Condition : Off`
		`Attention Condition : Off`
		`Locator LED : Off`
		
		`-> Command successful.`
		
		`MP Host Name: hqiasle8`
		
		`MP:CM>`

MA: RETURN TO MAIN MENU

The MA command causes the MP to return to the non-mirrored Main Menu. It is the same as executing the **Ctrl-B** command from the keyboard. EXIT is an alias for this command.

Menu-Based and Command Line Interfaces

Both command formats produce the same result:

```
MP Host Name: hqmaess2
MP:CM> MA
   MP MAIN MENU:
     CO: Consoles
     VFP: Virtual Front Panel
     CM: Command Menu
     CL: Console Logs
     CSP: Connect to Service Processor
     SE: Create Local Session
     SL: Show chassis Logs
     HE: Main Menu Help
     X: Exit Connection
MP Host Name: hqmaess2
MP:CM>
```

XU: MP FIRMWARE UPDATE (FW Command)

The XU command activates the upgrade mode. It serves as an alias for the FW command. It is only available from the LAN port and the local serial port.

Upgrade is performed through the MP LAN by FTP, which must therefore be operational. Information required for the upgrade needs to be entered through the FW command interface.

If the upgrade process, when started, is interrupted at any time, the core I/O will need to be repaired or replaced! The MP is reset at the end of the upgrade process.

2 Management Processor Card Firmware Upgrade

Introduction

This document is intended to provide information on the supported operating environment for MP and to provide installation instructions for upgrading the MP Processor Card Firmware to the latest release:

- The procedure for determining your current Management Processor Card Firmware version is described.
- The procedure for upgrading the MP Processor Card Firmware is explained.
- The procedure for setting up and using SSL is described.

Determining the Firmware Version

Please review all instructions and the Hewlett-Packard Support Tool License Terms, or your Hewlett-Packard support terms and conditions for precautions, scope of license, restrictions, and limitation of liability and warranties, before installing this patch.

It is important that you read and understand these instructions completely before you begin. This can determine your success in completing the Firmware update.

CAUTION The MP Card firmware upgrade process can only be done using an FTP site. For example, if the currently installed firmware is older than E.02.10, then updating to GSP firmware revision E.02.22 requires updating to E.02.10 first.

Finding the Current Firmware Version

The current version of the firmware must be E.02.10 or greater before this upgrade may be applied. If your firmware is older than E.02.10, apply the E.02.10 firmware upgrade first before applying any other upgrade. To find the current version of your firmware, complete the following steps:

Step 1. Establish a telnet session with the Management Processor.

Step 2. Log on to the Management Processor using the Admin password.

Step 3. Type **`^Ecf`** to get console write access, where ^E = CTRL key + e are pressed simultaneously.

Step 4. Type **`^b`** to enter the Management Processor, where the CTRL key + b are pressed simultaneously.

Step 5. Type **`HE`** at the MP> prompt.

A line similar to the following is displayed.

```
Hardware Revision e1  Firmware Revision E.02.20
```

Unpacking the Firmware

Before unpacking this upgrade, verify that the MP Firmware version is at E.02.10 or above and that the FTP server is available. Instructions are provided for unpacking the firmware on HP UX /Linux Red Hat and Windows systems.

Unpacking the Firmware on an HP UX /Linux Red Hat System

To unpack the firmware on an HP-UX system, complete the following steps:

Step 1. FTP the compressed file to an empty directory on an FTP server.

Step 2. Use **gunzip** to unzip the patchgunzip compressed file.

Step 3. Use the **tar** command to extract the firmware files. `# tar -xvf *tar`

```
x E0222.bin, 2453880 bytes, 4793 tape blocks
x Resources.out, 858965 bytes, 1678 tape blocks
x mp_upg.cnf, 201 bytes, 1 tape blocks
x version.dat, 16 bytes, 1 tape blocks
```

Step 4. Verify the checksum of the files by using the `cksum` command. Results of the command should be equal to the shown output example.

```
# cksum *
     1071770454 2453880 E0222.bin
     271796263 858965 Resources.out
     1334918069 201 mp_upg.cnf
     397171541 16 version.dat
```

Unpacking the Firmware on a Windows System

The procedure describes unpacking the files with WinZip. WinZip may be downloaded from www.winzip.com. To unpack the files on a Windows based system, complete the following steps:

Step 1. Save the compressed file to an empty directory on an FTP server.

Step 2. Unzip the compressed file by double clicking on the saved file.

Step 3. When the archive contains one file, use WinZip to decompress it to a temporary folder.

Step 4. Open the file by clicking Yes.

Step 5. Extract the files by selecting Actions | Extract.

Step 6. In the Extract dialog box, specify the extract-to location, then click Extract.

Establishing the Network Connection

After downloading and extracting the files, connect to the FTP server to establish a telnet session with the Management Processor. Before updating the firmware, test the FTP server connection to ensure its validity and integrity before using it to perform the update.

To test the network connection to the FTP server, complete the following steps:

Step 1. Establish a telnet session with the Management Processor.

Step 2. Log on to the Management Processor using the Admin password.

Step 3. Type **^Ecf** to get console write access.

Step 4. Type **^b** to enter the Management Processor.

Step 5. Access the Diagnostic Menu by using the XD command.

```
GSP> xd
```

Step 6. Select 3 to Ping the LAN where the GSP files are located (LAN access PING):

```
Non destructive tests:
1. Parameters checksum
2. I2C access (get Power Monitor status)
3. LAN access (PING)
4. Modem selftests
5. Secondary I2C access (get System status)Type R to reset the GSP or [Q] to quit the diagnosti
c menu.

Choice: 3

Enter IP Address: (Enter the IP address of the FTP server)>
```

This test must be passed by the server being used to supply the update files.

Step 7. Reset the GSP by entering the R option of the XD command.

```
-> Choice: r

      The MP is now being reset...
```

This frees up any unallocated memory for the GSP update.

Install the MP Firmware

Once the FTP server connection has been tested and the existing firmware version has been validated to be at E.02.10 or above, complete the following steps to update the currently installed firmware:

Step 1. Log on to the Management Processor using the Admin password.

Step 2. Type **^Ecf** to get console write access.

Step 3. Type **^b** to enter the Management Processor.

Step 4. Select the GSP command XU. This command activates the upgrade mode.

Step 5. Update the GSP firmware to the firmware image in the upgrade directory:

```
GSP> xu

XU
This command activates the upgrade mode. All connections will be closed, the session will be ab
orted and the modem connection will be dropped immediately, web and telnet connections will be
dropped upon completion.
Please, confirm your intention to activate the upgrade mode (Y/[N]) : y

Enter source system IP address: (Enter the IP address of the FTP server)
Enter file path: (Enter the Full Absolute path to the E.02.22 Directory)
Do you wish to use the default login: anonymous / GSP@hp.com (Y/[N]) :
y (if using anonymous FTP)
```

```
n (if using not using anonymous FTP).
IE: if root then supply root password
-> GSP firmware upgrade in progress ...
Retrieved an upgrade file successfully.
Programming ROM.  Percent Complete: 100.
Retrieved an upgrade file successfully.
Programming ROM.  Percent Complete: 100.
Retrieved an upgrade file successfully.
Programming ROM.  Percent Complete: 100.
-> GSP firmware upgrade complete - Web and telnet connections will be dropped.  GSP will now re
set....
Firmware installation is complete.

Due to PCI changes this firmware update requires the removal of AC power to the system.
```

Step 6. Remove the AC power cord for at least fifty-five seconds.

Step 7. Plug in the AC power cord and reboot the system.

This completes the firmware upgrade procedure.

Using SSL

SSL allows secure connections to MP using a browser. To use SSL, you must have previously generated a certificate.

The MP uses RSA libraries to implement the SSL protocol. SSL uses the following encryption standards:

- 1024-bit SSL and 128-bit RC4 encryption of web console data.
- RSA keys stored in ANS1 format.
- SSL key is 1024 bits.
- SSL uses an X509 Certificate stored in ANS1 format.

Setting Up SSL

To use SSL, the following actions must be taken:

- Activate SSL
- Generate a certificate
- Reboot MP to start browsing as an HTTPS server

Activate SSL

To activate SSL, complete the following steps:

Step 1. From the web console, enable SSL using the `SO` command.

Step 2. Generate a certificate by using the `CG` command.

Generate a Certificate

To generate a certificate, complete the following steps:

Step 1. Type **`CG`** at the MP command handler. If you have a certificate, the expiration date should be shown.

Step 2. The command displays the current certificate parameters. Enter or edit any information desired. Press **Enter** when editing is completed.

Step 3. The firmware generates *both* a key and certificate. It is not necessary to generate a key independently. This command takes several minutes to complete.

The `CG` command instructs you to restart the GSP and the browser.

Step 4. Reset GSD using the `R` option of the `XD` command: **`XD -R`**

Step 5. Exit all sessions of your browser.

Using the Secure Connection

The browser used for accessing the secure connection must have the following capabilities:

- SSL version 3 enabled
- Support 1024 bit encrypted certificates

- Support and have enabled Java plugin 1.3.1_06

To connect to the MP using the HTTPS, complete the following steps:

Step 1. Start your browser.

Step 2. Access the web console via the secure url: **`https://ipofgsp/`**

Step 3. Accept the certificate. You may now access the GSP from any browser from which you have accepted a certificate.