Cisco C880 M4 Server
Administration Manual
for Servers with E7-8800 v2 and E7-8800 v3 CPUs

November, 2015

Contents

CHAPTER 1 Network Environment Setup and Tool Installation 1
1.1 External Network Configuration 1
1.2 How to Configure the External Networks (Management LAN/ Maintenance LAN/Production LAN) 2
1.2.1 IP addresses used in the Cisco C880 server 2
1.3 Management LAN 3
1.3.1 How to configure the management LAN 3
1.4 Maintenance LAN 6
1.5 Production LAN 6
1.5.1 Overview of the production LAN 6
1.6 Management Tool Operating Conditions and Use 6
1.6.1 MMB 6
1.6.2 Remote operation (BMC) 7
CHAPTER 2 Component Configuration and Replacement (Add, Remove) 22
2.1 High availability configuration 22
2.1.1 Memory Operation Mode 22
2.1.2 Memory Mirror 23
2.1.3 Hardware RAID 26
2.1.4 Cluster configuration 26
2.2 Replacing components 26
2.2.1 Replaceable components 26
2.2.2 Component replacement conditions 27
2.2.3 Replacement procedures in cold maintenance 27
2.2.4 Replacing the battery backup unit of the uninterrupted power supply unit (UPS) 28
2.2.5 Replacing the PCI SSD card 28
2.3 Expansion of components 29
CHAPTER 3 Replacement of HDD/SSD 31
3.1 Hot replacement of HDD/SSD with Hardware RAID configuration 31
3.1.1 Hot replacement of failed HDD/SSD with RAID0 configuration 31
3.1.2 Hot replacement of failed HDD/SSD with RAID 1, RAID 1E, RAID 5, RAID 6, or RAID 10 configuration 31
3.2 Preventive replacement of HDD/SSD with Hardware RAID configuration 32
3.2.1 Preventive replacement of failed HDD/SSD with RAID0 configuration 32
3.2.2 Preventive replacement of failed HDD/SSD with RAID 1, RAID 1E, RAID 5, RAID 6, or RAID 10 configuration 33
3.3 Replacement of HDD/SSD in case hot replacement cannot be performed 34
CHAPTER 4 Backup and Restore 35
4.1 Backing Up and Restoring Configuration Information 35
4.1.1 Backing up and restoring UEFI configuration information 35
4.1.2 Backing up and restoring MMB configuration information 35
CHAPTER 5 Chapter System Startup/Shutdown and Power Control 37
5.1 System Power on and Power off 37
5.1.1 Various Methods for Powering On the System 37
5.1.2 Types of Power off Method of System 37
5.1.3 Procedure for System Power On and Power Off 38
5.1.4 System Power on by MMB 38
5.1.5 Checking the System Power status by using the MMB 38
5.1.6 Powering off the system by using the MMB 38
5.2 Scheduled operations 38
5.2.1 Powering on the system by scheduled operation 38
5.2.2 Power off the system by scheduled operation 39
5.2.3 Relation of scheduled operation and power restoration function 39
5.2.4 Scheduled operation support conditions 39
5.3 Automatic System Restart Conditions 40
5.3.1 Setting automatic system restart conditions 40
5.4 Power Restoration 40
5.4.1 Settings for Power Restoration 41
5.5 Remote shutdown (Windows) 41
5.5.1 Prerequisites for remote shutdown 41
5.5.2 How to use remote shutdown 42
CHAPTER 6 Error Notification and Maintenance (Contents, Methods, and Procedures) 43
6.1 Maintenance 43
6.1.1 Maintenance using the MMB 43
6.1.2 Maintenance method 43

6.1.3 Maintenance modes 43
6.1.4 Maintenance of the MMB 44
6.2 Troubleshooting 44
6.2.1 Troubleshooting overview 44
6.2.2 Items to confirm before contacting a sales representative 46
6.2.3 Finding out about abnormal conditions 46
6.2.4 Investigating abnormal conditions 48
6.3 Notes on Troubleshooting 49
6.4 Configuring and Checking Log Information 49
6.4.1 List of log information 49
6.5 Firmware Updates 49
6.5.1 Notes on updating firmware 49
Appendix A Functions Provided by the Cisco C880 server 50
A.1 Function List 50
A.1.1 Action 50
A.1.2 Operation 50
A.1.3 Monitoring and reporting functions 51
A.1.4 Maintenance 52
A.1.5 Redundancy functions 52
A.1.6 External linkage functions 53
A.1.7 Security functions 53
A.2 Correspondence between Functions and Interfaces 53
A.2.1 System information display 53
A.2.2 System settings 54
A.2.3 System operation 54
A.2.4 Hardware status display 54
A.2.5 Display of system configuration information 54
A.2.6 System configuration and operation setting 55
A.2.7 System operation 55
A.2.8 System power control 55
A.2.9 OS boot settings 55
A.2.10 MMB user account control 55
A.2.11 Server management network settings 56
A.2.12 Maintenance 56
A.3 Management Network Specifications 56
Appendix B Physical Mounting Locations and Port Numbers 58
B.1 Physical Mounting Locations of Components 58
B.2 Port Numbers 59
Appendix C Lists of External Interfaces Physical 61
C.1 List of External System Interfaces 61
C.2 List of External MMB Interfaces 61
Appendix D Physical Locations and BUS Numbers of Built-in I/O, and PCI Slot Mounting Locations and Slot Numbers 62
D.1 Physical Locations and BUS Numbers of Internal I/O Controllers of the Cisco C880 server 62
D.2 Correspondence between PCI Slot Mounting Locations and Slot Numbers 62
Appendix E Status Checks with LEDs 64
E.1. LED Type 64
E.1.1 Power LED, Alarm LED, and Location LED 64
E.1.2 PSU 64
E.1.3 FANU 65
E.1.4 SB 65
E.1.5 IOU 65
E.1.6 PCI Express slot of IOU 66
E.1.7 DU 66
E.1.8 HDD/SSD 66
E.1.9 MMB 67
E.1.10 LAN 67
E.1.11 OPL 67
E.2 LED Mounting Locations 68
E.3 LED list 71
Appendix F Component Mounting Conditions 74
F.1 CPU 74
F.2 DIMM 74
F.3 Available internal I/O ports 76
F.4 Legacy BIOS Compatibility (CSM) 76
F.5 NIC (Network Interface Card) 76

Appendix G Failure Report Sheet 78
G.1 Failure Report Sheet 78

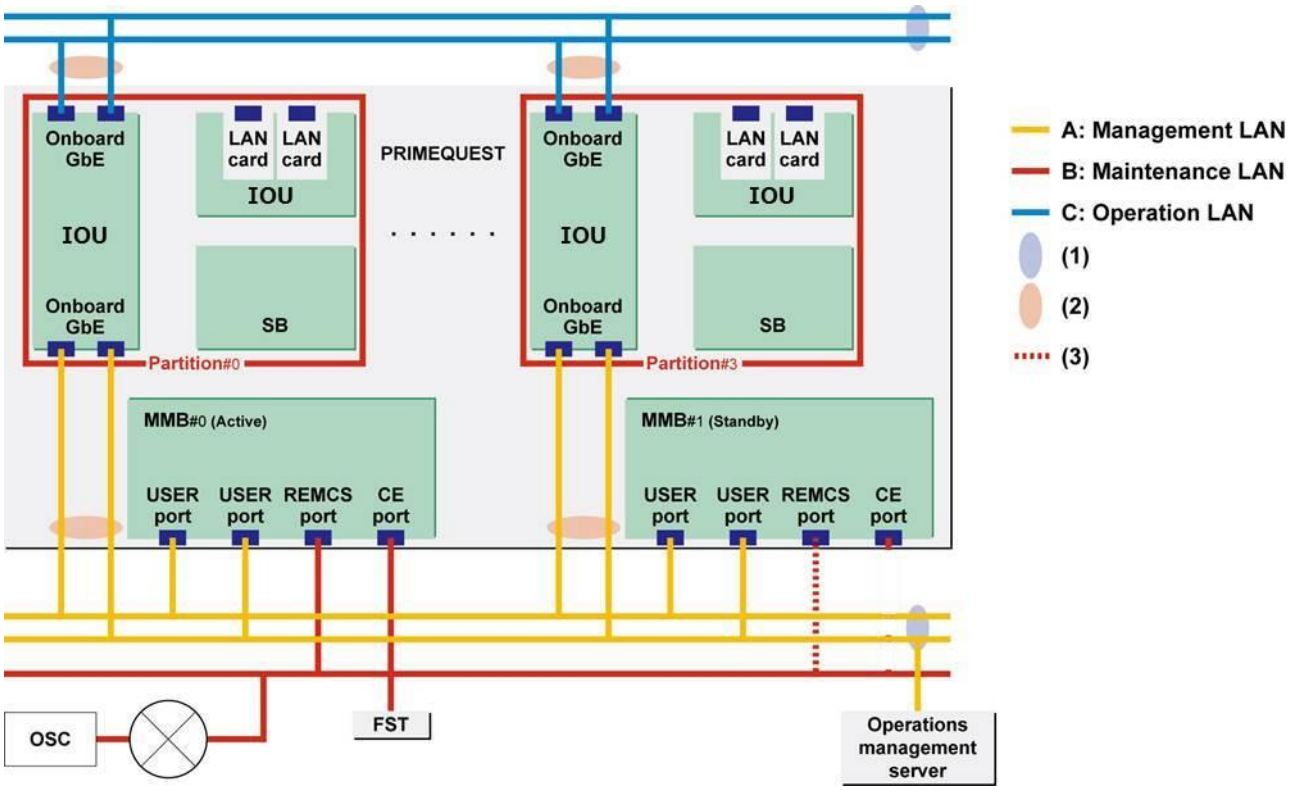
CHAPTER 1 Network Environment Setup and Tool Installation

This chapter describes the external network environment and management tool installation for the Cisco C880 server.

1.1 External Network Configuration

The following diagram shows the external network configuration for the Cisco C880 server.

FIGURE 1.1 External network configuration



No.	Description
(1)	SW redundancy
(2)	Redundancy by teaming

The following table lists the external networks. The letters A, B, and C correspond to those in FIGURE 1.1 External network configuration.

TABLE 1.1 External network names and functions

Letter	External network name	Function
A	Management LAN	- MMB Web-UI/CLI operations - Operations management server - Video redirection
B	Maintenance LAN	- FE terminal connection
C	Operation LAN (production LAN)	For job operations

1.2 How to Configure the External Networks (Management LAN/ Maintenance LAN/Production LAN)

The Cisco C880 server must be connected to the following three types of external networks. The respective external networks are dedicated to security and load distribution. (See FIGURE 1.1 External network configuration.)

- Management LAN
- Maintenance LAN
- Production LAN

Note
Be sure to connect management LAN, production LAN and maintenance LAN to different subnet each other

This section describes the IP addresses for the Cisco C880 server.

1.2.1 IP addresses used in the Cisco C880 server

Each of the SB, IOU, and MMB units in the Cisco C880 server has network interfaces. Each port of these network interfaces must be assigned an IP address.
To the ports, assign IP addresses appropriate to the external network environment of the Cisco C880 server. The following describes the IP addresses assigned to the ports.
TABLE 1.2 IP addresses for the Cisco C880 server (IP addresses set from the MMB) lists the IP addresses that are set from the MMB. TABLE 1.3 IP addresses for the Cisco C880 server (set from the operating system) lists the IP addresses that are set from the operating system.
The IP addresses in TABLE 1.2 IP addresses for the Cisco C880 server (IP addresses set from the MMB) are assigned to the NICs (network interface controllers) on the MMBs. Each NIC is connected to an SB or an external network port of the MMB through the switching hub on the MMB. The MMB firmware uses the IP addresses.

TABLE 1.2 IP addresses for the Cisco C880 server (IP addresses set from the MMB)

Name	NIC	Type	IP address setting method	Description
- Management LAN IP address: MMB Physical IP address This IP address is used for communication when the MMB is connected to the management LAN. The physical IP address is assigned to the NIC of the user port of MMB.				
MMB IP Address	MMB	Physical IP address	Set it from the MMB CLI or MMB Web-UI.	The PC connected to the management LAN uses this IP address to communicate with MMB.
- Maintenance LAN IP address: Maintenance IP address This IP address is used for communication when the MMB is connected to the maintenance LAN.				
Maintenance IP Address	MMB (common)	Physical IP address	Set it from the MMB CLI or MMB Web-UI.	This IP address is used for CE port.
- Console redirection IP address: Console Redirection IP Address				
Console Redirection IP Address	BMC	Physical IP address (*2)	Set it from the MMB Web-UI.	This IP address is used to access the console redirection function in the system from the PC on the management LAN.

*1 This IP address is to access the console redirection function provided by BMC. It accesses BMC from the user port on the management LAN of MMB via the dedicated network for BMC-to-MMB communication inside the cabinet.
MMB changes the local IP address of BMC to the IP address on the management LAN by NAT. From the PC on the management LAN, the console redirection function of BMC is used via MMB.

Remarks

- A separate subnet must be assigned to "Management LAN", "Maintenance LAN" (external network), and "Internal LAN" (inside the cabinet LAN).
- Since "Internal LAN" is closed to the outside of the cabinet, the same subnet as that for "Internal LAN" in another cabinet can be used.
- For the IP address to be assigned to "Console redirection", the same subnet as that assigned to "1. Management LAN" must be used.
- MMB uses the following subnets permanently for internal communication.
  The following subnets cannot be specified:
  127.1.1.0/24
  127.1.2.0/24
  127.1.3.0/24

TABLE 1.3 IP addresses for the Cisco C880 server (set from the operating system)

LAN port	IP address setting method	Description
LAN port in IOU	Set it from the OS in the system.	This depends on the system configuration.
Network card mounted in PCI Express slot in IOU.	Set it from the OS in the system.	Each port is connected to a network outside the cabinet. The ports in the system must have IP addresses. (Assign IP addresses to the ports used for actual operation.)

Remarks

- Only “AutoNego” is supported as setting of GbE port speed in IOU_10GbE.

1.3 Management LAN

This section describes the configuration of the management LAN for the Cisco C880 server.

1.3.1 How to configure the management LAN

The network for MMB access from external terminals is the management LAN.
For management LAN-related settings for MMB access, use the CLI or the [Network Configuration] menu in the Web-UI. For details on the network configuration, see 1.1 External Network Configuration.
The following lists the settings for the management LAN configuration. Only a user with Administrator privileges can make management LAN-related settings.

TABLE 1.4 Parts of the management LAN configuration

Display/Setting item	Description
Network Interface: IP address and other settings for MMB access	
MMB IP Address	Physical IP address of MMB. You set this IP address for MMB. Enable/Disable setting Interface Name/IP Address/Subnet Mask/Gateway Address
DNS (optional)	Option. It specifies the IP address of the DNS server used. The default is ‘Disabled’. Enable/Disable setting IP Address: DNS Server 1/DNS Server 2/DNS Server 3
Management LAN	Specifies duplication of the management LAN ports. The default is ‘Disabled’. (Only the ports on the #0 side are enabled.) Enable/Disable setting
Maintenance IP Address	Specifies the CE port. The default is ‘Disabled’. Enable/Disable setting IP Address/Subnet Mask/SMTP Address
Management LAN Port Configuration: Management LAN port settings	
Speed/Duplex for MMB	Specifies a Speed/Duplex value for the MMB LAN ports. Port: USER Port, Maintenance Port Setting value: Auto (default), 100M/Full, 100M/Half, 10M/Full, 10M/ Half The MMB USER port is duplicated. The possible settings for the respective ports depend on the MMB hardware configuration.
Network Protocols: Network protocol settings	
HTTP, HTTPS, telnet, SSH, SNMP	Specifies whether to enable or disable a protocol, the port number, and the Timeout time.

Display/Setting item	Description
SNMP Configuration: SNMP-related settings	
SNMP Community	Specifies SNMP System Information and Community/User values. - System Information: Specifies System Location and System Contact values for SNMP. It also displays the system name specified from [System] - [System Information]. - Community: Can specify up to 16 Community/User items. Each Community/User item includes the access-permitted IP address, SNMP version, access permission, and authentication settings. For settings specific to SNMP v3, use the SNMP v3 Configuration menu.
SNMP Trap	Specifies SNMP trap destinations. You can set up to 16 destinations. Each trap destination item includes the Community/User name, destination IP address, SNMP version, and authentication level settings. - [Test Trap] button: Sends a test trap to the specified trap destination.
SNMP v3 Configuration: Settings specific to SNMP v3	
Engine ID	Specifies the Engine ID. - Enter the encryption hash function, authentication passphrase, and encryption passphrase for users.
SSL: SSL settings	
Create CSR	Creates a private key and a request for a signature (CSR: Certificate Signing Request) - SSL certificate status: Displays the current status of SSL certificate installation. - Key length: Length of the private key, 1024 bits or 2048 bits - Entered information on the owner specified for the CSR - Country, prefecture, city/town, organization, department, server, e-mail address - [Create CSR] button: Displays a confirmation dialog box. Clicking [OK] creates a new private key and a request for a signature. After completion, a dialog box appears. Clicking [OK] registers the private key and causes a jump to the [Export Key/CSR] window. Clicking [Cancel] gives an instruction to discard the created private key and CSR.
Export Key/CSR	Exports an MMB private key/CSR (backup). - [Export Key] button: Exports a private key. - [Export CSR] button: Exports a CSR. **Note** Clicking the [Export Key] button/ [Export CSR] button using FireFox 4 or later flashes a save confirmation dialog box, resulting in the secret key not being downloadable. Therefore, use Internet Explorer during [Export Key/Export CSR] window manipulation.
Import Certificate	Imports a signed electronic certificate sent from a certificate authority. To import a file, specify the file, and click the [Import] button.
Create Selfsigned Certificate	Creates a self-signed certificate. - SSL certificate status: Displays the current status of self-signed certificate installation. - Term: Specifies the term of validity (number of days) of the self-signed certificate. - The other settings are the same as on the [Create CSR] window. - [Create Selfsigned Certificate] button: Creates a self-signed certificate.
SSH: SSH settings	
Create SSH Server Key	Creates an SSH server private key. - SSH Server Key Status: Displays the status of SSH server key installation. - [Create SSH Server Key] button: Creates a private key. After creation is completed, a confirmation dialog box appears. Clicking [OK] installs the created key. Clicking [Cancel] discards it.
Remote Server Management: User settings for remote control of the MMB via RMCP - Use the [Edit User] button to select the user to be edited. The default settings for all users is [No Access] and [Disable]. - You can edit the user name, password, permission, and status (Enable/Disable) in the [Edit User] - To deny access to a user, set [No Access] for permission or [Disable] for [Status].	
Access Control: Access control settings for network protocols	

Display/Setting item	Description
[Add Filter]/[Edit Filter]/ [Remove Filter] button	Adds, edits, or deletes a filter.
[Edit Filter] window	- Protocol: Select the target protocol (HTTP/HTTPS/telnet/SSH/SNMP). - Access Control: Select [Enable] or [Disable]. - Disable: Denies access by any IP address. - Enable: Permits access by only the specified IP addresses. - IP Address/Subnet Mask: You can specify this item only if the [Access Control] setting is [Enable]. The filtering permits access by only the IP addresses specified here.
Alarm E-Mail: Settings for e-mail notification of an event	
Alarm E-Mail	Used to select whether to send e-mail for the occurrence of an event (Enable/ Disable).
From	Sender address
To	Destination address
SMTP Server	IP address or FQDN of the SMTP server
Subject	E-mail title
[Filter] button	Used to edit Alarm E-mail transmission filter settings. The occurrence of any event specified in the filter settings is reported by e-mail. The default for target events is all events. - Severity: Target severity (Error/Warning/Info) - Unit: Target unit - Source: Target source (CPU/DIMM/Chipset/Voltage/Temperature/ Other)
[Test E-Mail] button	Sends test e-mail.
Video redirection/remote storage network settings	
[System] - [Console Redirection Setup] menu	The video redirection/remote storage network relays traffic through the MMB, so the BMC IP address is not seen by users. Users access the system via the management LAN of the MMB. Here, specify the IP address used for access by the video redirection client (Java applet). The MMB handles address conversion between the specified address and BMC IP address.

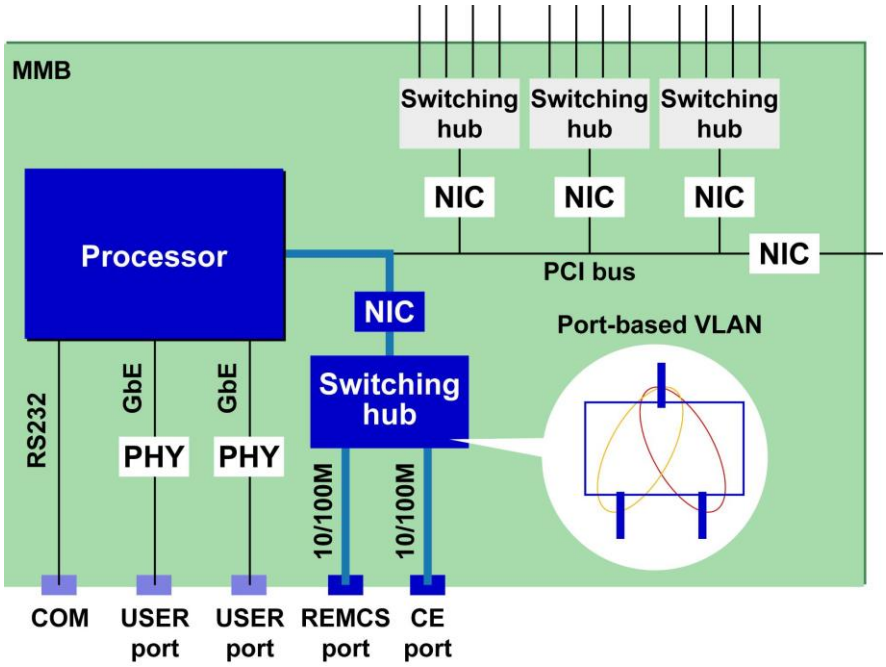
1.4 Maintenance LAN

The MMB provides the following LAN ports for maintenance purposes.

TABLE 1.5 Maintenance LAN

Port	Description	Remarks
CE LAN	CE terminal port for use in maintenance work	100Base-TX, RJ45
REMCS LAN	This port is not used.	100Base-TX, RJ45

FIGURE 1.2 Maintenance LAN of the MMB



The maintenance LAN is configured with Web-UI or CLI of the MMB. The subnet of the maintenance LAN must be separated from the other subnets such as one for the management LAN, the production LAN, etc.

Remarks

Maintenance IP can pass beyond only one gateway with specified address.

1.5 Production LAN

This section describes the configuration of the production LAN for the Cisco C880 server.

1.5.1 Overview of the production LAN

The IOU includes LAN ports for the production LAN.
You can mount additional LAN cards in the PCI Express slots on the IOU as needed, to use their ports for the production LAN.

1.6 Management Tool Operating Conditions and Use

This section describes the operating conditions and use of the management tools.

1.6.1 MMB

The MMB Web-UI operating conditions are as follows.

Supported Web browsers

Firefox version 20 or later (operating system: Windows or Linux)
Internet Explorer version 9 or later (operating system: Windows)

Maximum number of Web-UI login users

Up to 16 users can log in to the Web-UI at a time. If 16 users have logged in when another user attempts to log in, a warning dialog box appears and the login attempt is rejected.
The MMB Web-UI login procedure is as follows.

1. Specify the URL of the MMB in the Web browser to connect to the MMB.
   >> The [Login] window appears.
2. Enter your user name and password.
   >> The [Web-UI] window ([System] - [System Status]) appears.

MMB user privileges

User privileges specify the levels of MMB operating privileges held by user accounts.
Only users with Administrator privileges can create, delete, and modify user accounts.

NTP client function setting on the MMB

In the Cisco C880 server, the MMB acts as an NTP client to ensure synchronization with external NTP servers.

1.6.2 Remote operation (BMC)

Supported Web browsers

Firefox version 20 or later (operating system: Windows or Linux)
Internet Explorer version 9 or later (operating system: Windows)

Required Java Runtime Environment

Java 6 or later
Notes

- For a terminal whose operating system is Windows Vista or later and Windows Server 2008 or later, set UAC (User Account Control) or UAP (User Account Protection) to "Disabled" or start the browser as administrator privilege.
- For video redirection and virtual media, a connection may not be established if the network is connected via a proxy. In such cases, change the browser setting to avoid network connection via the proxy. If you still cannot establish a connection, perform the setting used for direct connection for Java network.
- To start the video redirection function with Internet Explorer, click the mouse while holding down the [Control] key. Even if the following message is displayed, click the mouse while holding down the [Control] key.
- Message displayed on the status bar of Internet Explorer
  "Pop-up blocked." (To allow the pop-up window to open, click the mouse while holding down the [Ctrl] key. With FireFox, you can establish a connection simply by clicking the mouse.
- If " java.net.SocketException: Malformed reply from SOCKS server" occurs when you attempt to establish a video redirection connection, make the following browser setting.
  - For Internet Explorer:
    1. Select [Tools] - [Internet Options] - [Connection] tab - [LAN Settings] - [Proxy Server] - [Advanced].
    2. Uncheck [Use the same proxy server for all protocols].
    3. Clear the Socks field.
  - For FireFox:
    1. Select [Tools] - [Options] - [Network] tab - [Connection Settings].
    2. Check [Manual proxy configuration].
    3. Uncheck [Use this proxy server for all protocols].

4. Clear the SOCKS field.

- Window may be maximized when you attempt to establish a video redirection connection or during video redirection connection. In such cases, change to window size suitable for environment of your terminal.

Maximum number of connections

The following lists the maximum number of connections using the remote operation (BMC) function.

TABLE 1.6 Maximum number of connections using the remote operation function

Item	Description
Video redirection	Up to 2 users can be connected concurrently. However, only 1 user can perform operations. The other user can only refer to information.
Virtual Media	Up to two devices can be connected for floppy, CD or DVD, Hard disk drive, independently.

The operating conditions for BMC installation of individual BMC functions is described below.

Operating environment settings

You need to make the appropriate settings for video redirection and virtual media for your network environment. In the [Console Redirection Setup] window of the MMB Web-UI, set the IP address and subnet mask, and set enable or disable for video redirection and virtual media.

Video redirection

With the video redirection function, users can access windows for the system side from a remote location. When a user starts video redirection from the [Console Redirection] window of the MMB Web-UI, a Java applet is sent to the user's terminal. Through the Java applet, the terminal displays VGA output sent to the LAN.
User input with the mouse or keyboard on the terminal is routed through the LAN to the system.
List of video redirection function is shown below.
Note

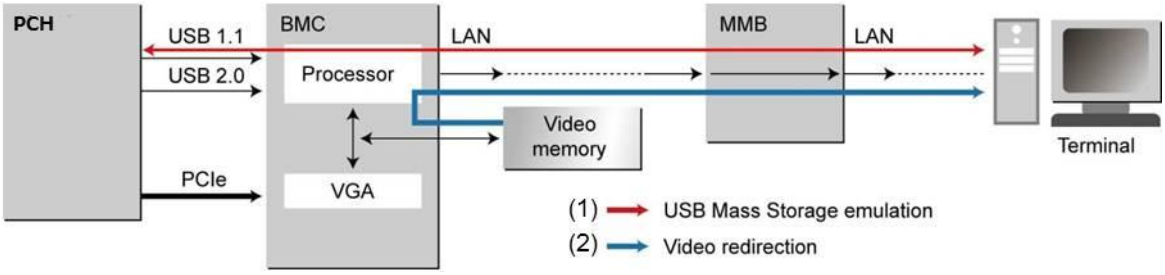
- If you cannot access to DNS server in the terminal for video redirection, do not set up the address of DNS server.

TABLE 1.7 List of video redirection function

Function	Description	Note
Window	Perform operation of screen display such as pause, zoom-in, zoom-out and language selection.	
Keyboard	Operate keyboard by keyboard of terminal PC.	Special key cannot be used directly.
Virtual keyboard	Display and operate virtual keyboard	
Mouse	Operate mouse by mouse of terminal PC. A mouse pointer in a system and a mouse pointer in a terminal PC run simultaneously. Display of mouse in a terminal PC can be set to enable or disable. Set position of mouse to ‘Absolute mode’. Default is ‘Absolute mode’.	
Special key	Send key operation of [Ctrl], [Alt], and [Windows] key. [Lock] key holds down the [Ctrl], [Alt], or [Windows] key.	
Power	Power on, power off, or re-start a system.	

The following shows a diagram of the connection configuration for video redirection.

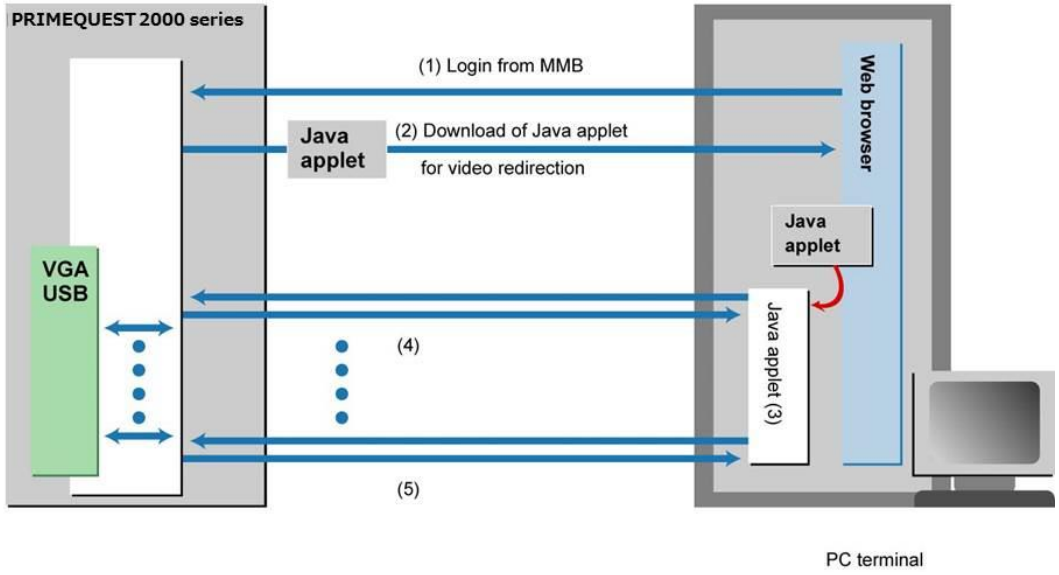
FIGURE 1.3 Connection configuration for video redirection



No.	Description
(1)	USB keyboard emulation and mouse emulation
(2)	Video redirection

The following shows the operating sequence of video redirection.

FIGURE 1.4 Operating sequence of video redirection



In the diagram, (1) to (5) indicates the following operations.

(1) Log in to the MMB Web-UI by browser.

(2) Display the window, and start video redirection.

(3) You can perform system operations from the [Video Redirection] window by using the keyboard and mouse.

(4) You can perform system operations through the Java applet for video redirection.

(5) Exit video redirection.

The following shows an example of the [Video Redirection] window.

FIGURE 1.5 [Video Redirection] window

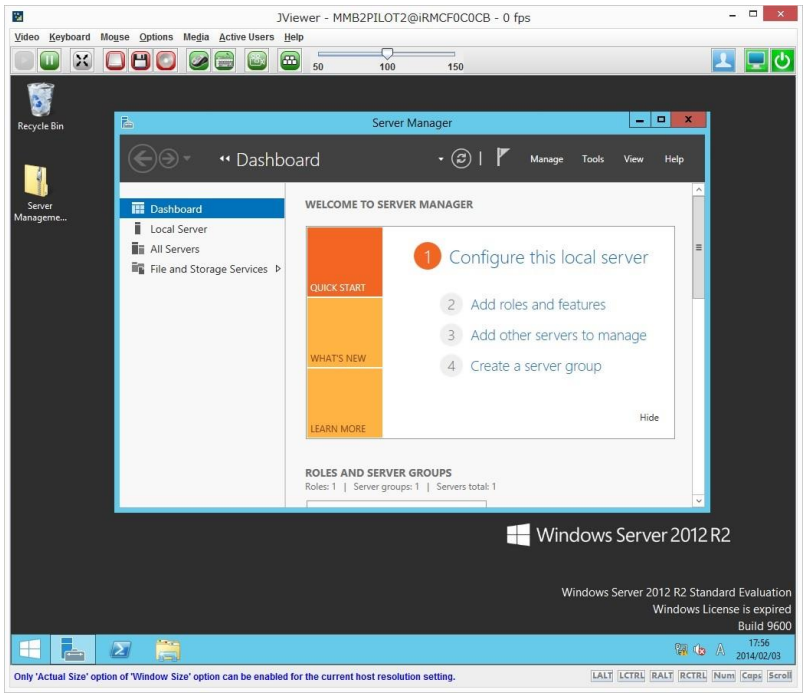


TABLE 1.8 Menu Bar in [Video redirection] window

Menu Bar			Description
Video			
	Pause Redirection		Perform pause of [Video redirection] window.
	Resume Redirection		Release pause of [Video redirection] window.
	Refresh Video		Refresh [Video redirection] window.
	Turn ON Host Display Video		Show video operation on host monitor.
	Turn OFF Host Display		Show video operation on host monitor.
	Low Bandwidth Mode		Set bits per pixel (bpp) of [Video redirection] window.
		Normal	Set ‘Normal’.
		8 bpp	Set ‘8 bpp’.
		8 bpp B&W	Set ‘8 bpp monochrome’.
		16 bpp	Set ’16 bpp’.
	Capture Screen		Capture [Video redirection] window. The screen is preserved into terminal PC in jpeg format.
	Full Screen		Maximize [Video redirection] window. It is required that client and host are the same resolution.
	Start Record		Start to record [Video redirection] window. The video is preserved into terminal PC in avi format.
	Stop Record		Stop to record [Video redirection] window.
	Settings		Perform setup for record of [Video redirection] such as record time and save location.
	Exit		Close video redirection.
Keyboard			
	Hold Right Ctrl Key		Hold down right [Ctrl] key. [RCTRL] button turns red.
	Hold Right Alt Key		Hold down right [Alt] key. [RALT] button turns red.
	Hold Left Ctrl Key		Hold down left [Ctrl] key. [LCTRL] button turns red.
	Hold Left Alt Key		Hold down left [Alt] key. [LALT] button turns red.
	Left Windows Key		
		Hold Down	Hold down [Windows] key.
		Press and Release	Press [Windows] key.
	Right Windows Key		

Menu Bar			Description
		Hold Down	Hold down [Windows] key.
		Press and Release	Press [Windows] key.
	Ctrl+Alt+Del		Press [Ctrl] key, [Alt] key, and [Del] key simultaneously.
	Context Menu		Open Context Menu (shortcut menu).
	Hot Keys		
		Add Hot Keys	Set Hot keys (shortcut key).
	Host Physical Keyboard		
		Auto Detect	Set to 'Auto Detect' Physical keyboard type is detected automatically.
		English(United States)	Set to 'English (United States)'.
		French	Set to 'French'.
		German(Germany)	Set to 'German'.
		Japanese	Set to 'Japanese'.
		Spanish	Set to 'Spanish'.
	SoftKeyboard		
		English(United States)	Set to 'English (United States)'.
		English(United Kingdom)	Set to 'English (United Kingdom)'.
		Spanish	Set to 'Spanish'.
		French	Set to 'French'.
		German(Germany)	Set to 'German (Germany)'.
		Italian	Set to 'Italian'.
		Danish	Set to 'Danish'.
		Finnish	Set to 'Finnish'.
		German(Switzerland)	Set to 'German (Switzerland)'.
		Norwegian(Norway)	Set to 'Norwegian'.
		Portuguese	Set to 'Portuguese'.
		Swedish	Set to 'Swedish'.
		Hebrew	Set to 'Hebrew'.
		French(Belgium)	Set to 'French (Belgium)'.
		Dutch(Belgium)	Set to 'French.'
		Russian(Russia)	Set to 'Russian'.
		Japanese(QWERTY)	Set to 'Japanese (QWERTY)'.
		Japanese(Hiragana)	Set to 'Japanese (Hiragana)'.
		Japanese(Katakana)	Set to 'Japanese (Katakana)'.
		Turkish - F	Set to 'Turkish -F'.
		Turkish - Q	Set to 'Turkish -Q'.
Mouse			
	Show Cursor		Display cursor.
	Mouse Calibration		Perform calibration of mouse location.
	Show Host Cursor		Display host cursor.
	Mouse Mode		
		Absolute mouse mode	Set a mouse to 'Absolute mode'. A mouse pointer in [Video redirection] window is adjusted to absolute value of a mouse pointer in terminal PC.
		Relative mouse mode	Set a mouse to 'Relative mode'. A mouse pointer in [Video redirection] window is adjusted to relative position calculated by difference from previous position of a mouse in terminal PC.
		Hide mouse mode (*1)	Set a mouse to 'Hide mode'. This mode should be used if action of a mouse pointer in [Video redirection] does not match with that in terminal PC.
Options			
	Keyboard/Mouse Encryption		Encrypts keyboard data and mouse data.
	Window Size		
		Actual Size	Return size of [Video redirection] window to normal size (100%).
		Fit to Client Resolution	Fit to resolution of client window.
		Fit to Host Resolution	Fit to resolution of host window.
	GUI Languages		
		DE - Deutsch	Set menu display to 'German'.

Menu Bar			Description
		EN - English	Set menu display to ‘English’.
		JA - 日本語	Set menu display to ‘Japanese’.
	Request Full Permission		Request ‘Full Virtual Console access’ which means the permission of the ‘full access’. This item is shown only if your permission is the ‘partial access’ where you can only see the screen mainly.
Media			
	Virtual Media Wizard		Set virtual media.
Active Users			
	:		Display user who is performing video redirection.
Power (*2)			
	Power On		Power on the system.
	Immediate Power Off		Power off the system immediately.
	Power Cycle		After powering off the sytem, power on the system again.
	Press Power Button		Press power button.
	Immediate Reset		Perform hardware reset.
	Pulse NMI		Issue NMI.
	Graceful Reset (Reboot)		Perform Graceful Reset (Reboot).
	Graceful Power off (Shutdown)		Perform Graceful Power off (Shutdown)
	Set Boot Options		Perform setup of Boot Options.
Help			
	About JViewer		Display version information. If you click the "About JViewer", it may take a few minutes to appear the dialog box that displays the JViewer information. You cannot operate the video redirection in the meantime. In such a case, please wait a while for the dialog box to appear, or stop the javaw.exe task in task manager and then restart the video redirection.
	Server Information		Display information of server.

(*1) Set mouse mode to ‘Hide mouse mode’ when operate LSI WebBIOS since action of cursor in LSI WebBIOS is adjusted to actual action of your mouse cursor.
When you use two displays to operate LSI WebBIOS in Legacy Mode, use primary display of monitor 1. If you set to ‘Hide mouse mode’ in secondary display of monitor 2, cursor does not run. Even if you set to ‘Hide mouse mode’, it is no problem to use primary display and operate UEFI.

TABLE 1.9 Tool Bar menu in [Video redirection] window

Tool bar	Description
[Resume Redirection]	Release pause of [Video redirection] window.
[Pause Redirection]	Perform pause of [Video redirection] window.
[Full Screen]	Maximize [Video redirection] window. It is required that client and host are the same resolution.
[Hard disk/USB]	Set virtual media.
[Floppy]	Set virtual media.
[CD/DVD]	Set virtual media.
[Cursor]	Display cursor.
[Softkeyboard]	Display software keyboard.
[Video Record]	Perform setup for record of [Video redirection] such as record time and save location.
[Hot Keys]	Set Hot keys (shortcut key).
[Zoom]	Zoom in or Zoom out [Video redirection] window.

TABLE 1.10 Status Bar in [Video redirection] window

Status Bar	Description
[LALT]	Hold down left [Alt] key. [LALT] button turns red.
[LCTRL]	Hold down left [Ctrl] key. [LCTRL] button turns red.
[RALT]	Hold down right [Alt] key. [RALT] button turns red.

Status Bar	Description
[RCTRL]	Hold down right [Ctrl] key. [RCTRL] button turns red.
[Num]	Hold down right [Num] key. [Num] button turns red.
[Caps]	Hold down right [Caps] key. [Caps] button turns red.
[Scroll]	Hold down right [Scroll] key. [Scroll] button turns red.

Note

- When resolution of window in server is 800 x 600, a part of window displayed in video redirection may luck or track of mouse cursor may remain during installing Linux.
- While the video redirection is being used, a warning message indicating that the digital signature is expired may be displayed. Since this warning message does not affect the operation of Java Application, click the [Execute] button. To avoid displaying this waning message every time the video redirection is connected, check the check box for [Always trust content from this publisher], and click the [Execute] button.
- Network communication problems between the terminal and Cisco C880 server may cause a session interruption, resulting in the [Video Redirection] window failing to respond to user operation. In such cases, the window cannot be closed normally. Reconnect to the network after forcibly ending the video redirection.
- If below problems occur while using video redirection, reconnect video redirection.
  - No response comes from video redirection and any operation cannot be performed.
  - Display of video redirection window remains black or 'No Signal'.
  - Error dialog of video redirection appears and any operation cannot be performed.
  - Window of video redirection is disconnected unintentionally.
- If you use RHEL6 or RHEL7, windows for various settings may not be displayed paritially because maximum resolution of display is 1024 x 768 when you connect to the partition by only video redirection. Set the resolution of display to higher than 1024 x 768 by following steps. Following steps show the procedure to set to 1600 x 1200 as an example.

  1. Execute init 3 to stop Xwindow.

```
# /sbin/init 3
```

  2. Execute Xorg -configure command to create xorg.conf.new

```
# Xorg –configure
```

  3. Execute cvt x y to create modeline (x, y: pixel number). 1600 x 1200 is set in following example.

```
# cvt 1600 1200
# 1600x1200 59.87 Hz (CVT 1.92M3) hsync: 74.54 kHz; pclk:
161.00 MHz Modeline "1600x1200_60.00"  161.00  1600 1712 1880
2160  1200 1203 1207 1245 -hsync +vsync
```

  4. Edit xorg.conf.new to add ModeLine to Section "Monitor".

```
Section "Monitor"
 Identifier   "Monitor0"
 VendorName   "Monitor Vendor"
 ModelName    "Monitor Model"
 ModeLine     "1600x1200_60.00"  161.00  1600 1712 1880 2160
1200 1203 1207 1245 -hsync +vsync
EndSection
```

  5. Change name of xorg.conf.new to xorg.conf, and put it in /etc/X11/xorg.conf
  6. Reboot the partition. After rebooting partition, resolution of display becomes 1600 x 1200.
     1600 x 1200 is added to choices of resolution in property of display.
     Note
     If you set higher resolution than default, response of video redirection becomes slower.

Below description is how to connect video redirection.

1. First terminal PC is connected to the system by video redirection with Full Virtual Console Access.
2. If you connect to the system by video redirection, a massage requesting permission to virtual console access appears in second terminal PC.

FIGURE 1.6 Message of requesting access to Virtual Console in second terminal PC

3. In first terminal PC, window where connection privilege of second terminal PC is selected appears. Select connection privilege from below.

   - Allow Virtual Console
     permit Full Virtual Console access where all operation of video redirection can be performed.
   - Allow only Video
     permit only video where display function of video redirection can be performed.
   - Deny Access
     deny access to video redirection.

   If thirty seconds passes, [Allow Virtual Console] is selected.

FIGURE 1.7 Popup window of [Virtual Console Sharing Privileges]

4. Popup which shows result selected by first terminal PC.

   - Display in first terminal PC.
     Such below window is displayed depending on result of selection except for [Allow only Video].

FIGURE 1.8 Popup for [Allow Virtual Console] in first terminal PC

FIGURE 1.9 Popup for TIMEOUT in first terminal PC

   - Display in second terminal PC.
     Result selected by first terminal PC is shown below in second terminal PC.

FIGURE 1.10 Popup for [Allow Virtual Console] in second terminal PC

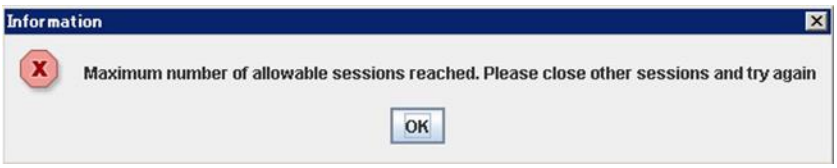
FIGURE 1.11 Popup for [Allow only video] in second terminal PC

FIGURE 1.12 Popup for [Deny Access] in second terminal PC

FIGURE 1.13 Popup for TIMEOUT in first terminal PC

- Display in third terminal
  If you try to open video redirection in third terminal PC, the dialog box instructing that connect again after closing other video redirection since the number of connection reaches the maximum of permitted number for video redirection.

FIGURE 1.14 Popup for reaching maximum number of connection in second terminal PC



Console redirection

Cisco C880 server provides console redirection to route serial output from the system via a LAN. Console redirection conforms to the specifications of IPMI v2.0 SOL (Serial Over LAN).
When you perform console command on MMB CLI, console output to the COM port on the system is redirected. Input from the terminal is reported to the COM port on the system.

Connection period of text console redirection

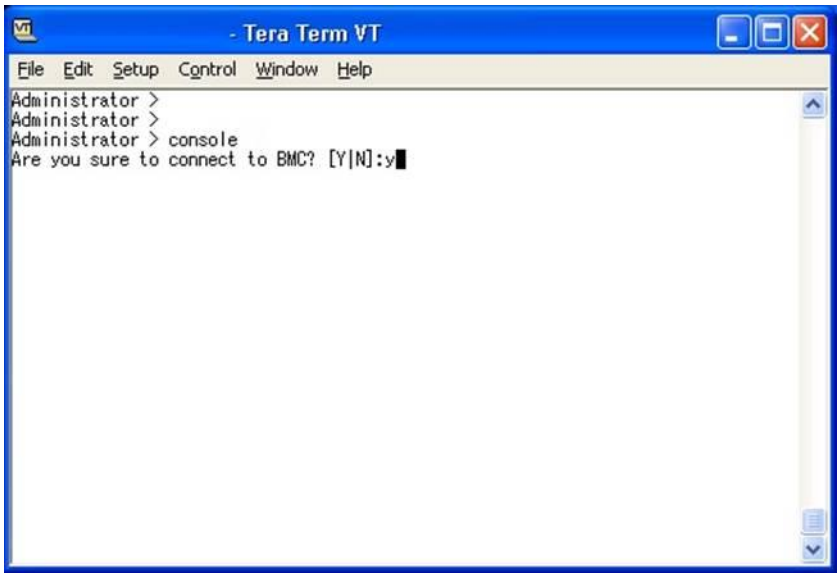
Console redirection is automatically disconnected after a certain idle time. You can set automatic disconnection time, timeout value, by console command.

How to connect console redirection

Note
If console redirection is disconnected due to timeout, below message appears.
“You have exceeded your idle time limit. Logging you off now.”

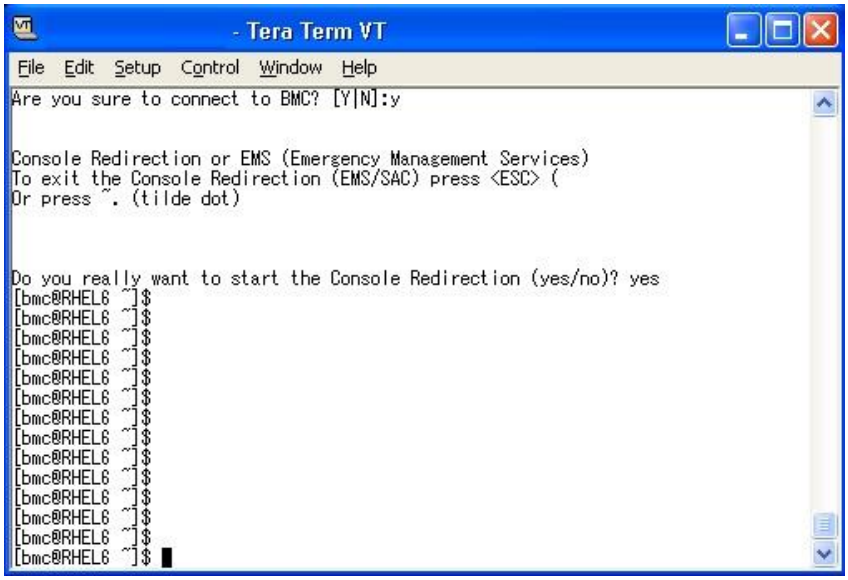
1. Login to MMB CLI and connect the system.
   If the message which confirms whether you connects or not appears, input ‘y’.

FIGURE 1.15 Example of setting (1)



2. If the message “Do you really want to start the Console Redirection (yes/no)?” appears, input ‘yes’. You can connect to the system.

FIGURE 1.16 Example of setting (2)



To close the console redirection, perform either of below operation:

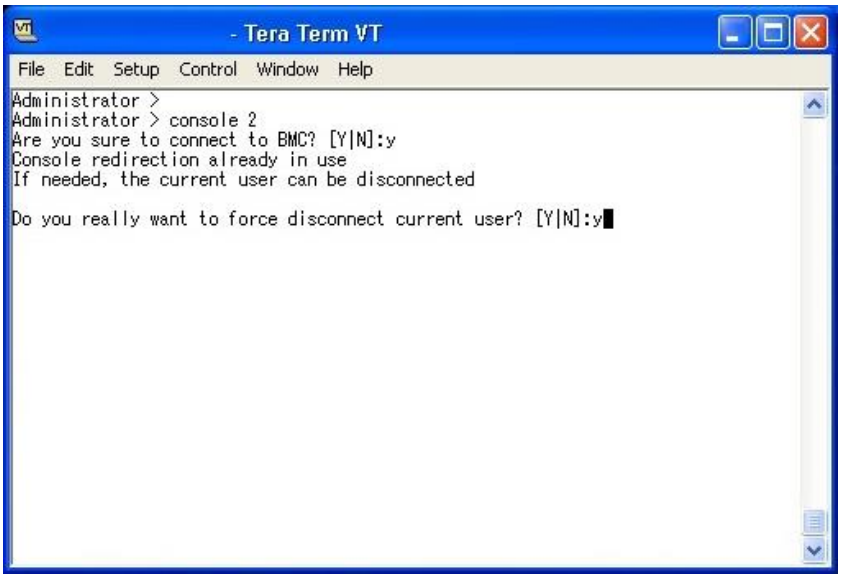
- Press [ESC] key and then press [(] key.
- Press [~] key and then press [.] key.

Forced disconnection of console redirection

Note
Only one user at a time is permitted to use the console redirection function.

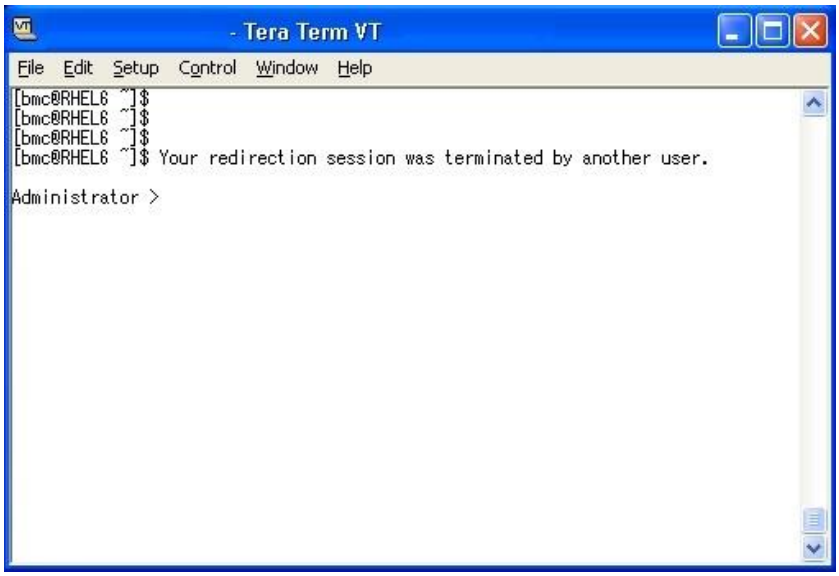
1. If a user attempts to connect using the function while another user is using it, the message "Console Redirection already in use" appears. The window appears as follows.

FIGURE 1.17 Forced disconnection of console redirection (1)



2. If you disconnect the console redirection of other user who has been already used, enter ‘yes’.
   You can use console redirection in place of current user.
   The terminal software of the disconnected user displays the following window.

FIGURE 1.18 Forced disconnection of console redirection (2)



Virtual Media

The virtual media function enables the system to share the floppy disk drives, CD or DVD drives, and HDD or USB devices of terminals as storage devices. For ISO images, ISO images on the terminal appear as emulated drives on the system side.
Up to two devices can be used per each device at the same time. Up to six devices can be used at same time in total.

Note

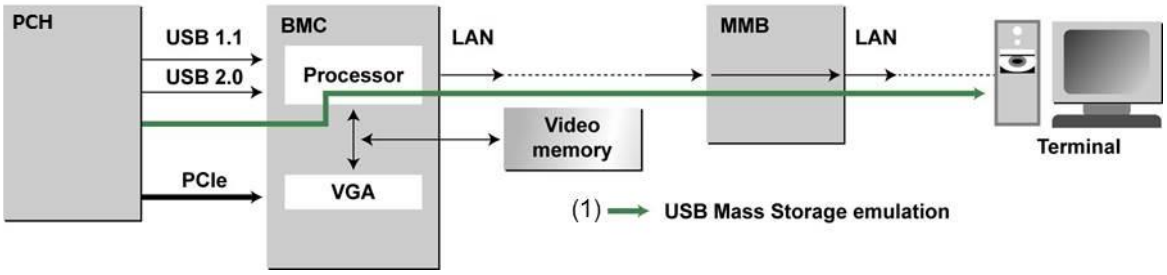
- For a terminal whose operating system is Windows Vista or later and Windows Server 2008 or later, set UAC (User Account Control) or UAP (User Account Protection) to "Disabled” or start the browser as administrator privilege.
- If the operation terminal is accessing the USB memory by using explorer and so on, the operation terminal does not recognize the USB as a connectable device by virtual media.

- You may receive a STOP error message on a blue screen when using the virtual media function from your terminal.
  The blue screen appears on the terminal under the following circumstances.
  - You are using the remote storage function from a terminal running one of the following Windows operating systems:
    - Windows XP
    - Windows Vista
    - Windows 7
    - Windows Server 2008 R2
    - Windows Server 2012
  - You are using two USB devices as remote storage devices.

This issue does not occur when only one USB device is used.
Example: One of your remote storage devices is a USB device and the other is an iso image.
If your terminal is running on Windows Vista or Windows Server 2008, you can avoid this issue by applying the hotfix from KB 974711. For details, see the Microsoft Knowledge Base.
If your terminal is running on Windows XP, Windows 7, or Windows Server 2008 R2, use only one USB device.
For more information related to Windows 7 or Windows Server 2008 R2, see the Microsoft Knowledge Base.

The following shows a diagram of the connection configuration for remote storage.

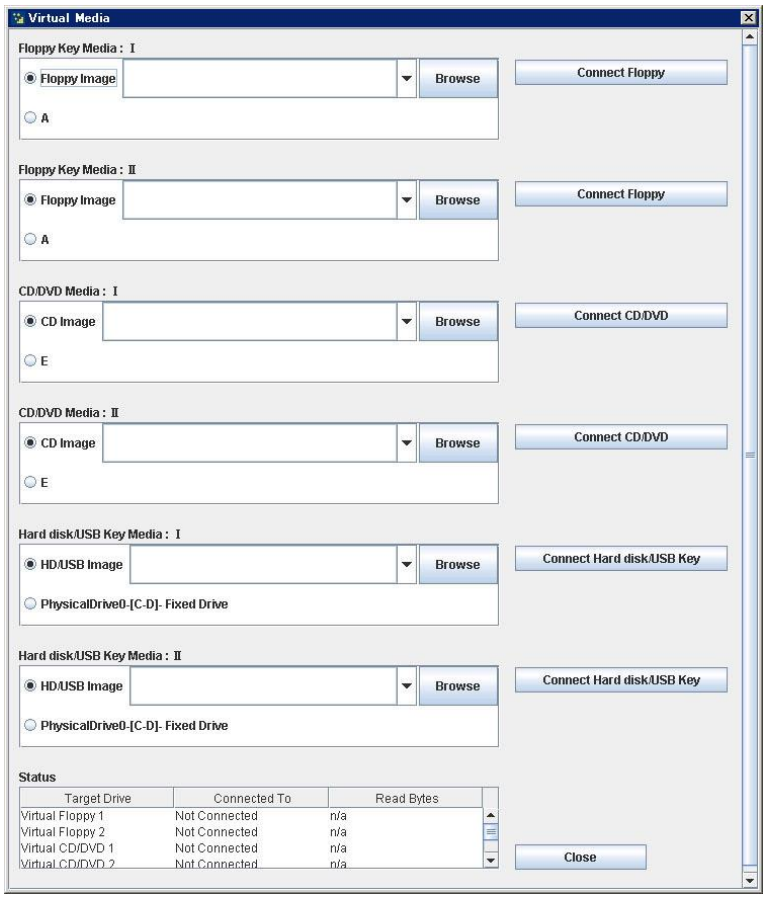
FIGURE 1.19 Configuration of virtual media connection



No.	Description
(1)	USB Mass Storage emulation

To recognize and display the devices that can be connected remotely, select [Virtual Media Wizard…] from the [Media] menu in the [Video Redirection] window. To recognize CD drives and DVD drives as devices that can be connected remotely, the drives must already have media inserted in them.

FIGURE 1.20 [Virtual Media] window (1)



The following lists the buttons available in the virtual media list window.

TABLE 1.11 Buttons in [Virtual Media] window

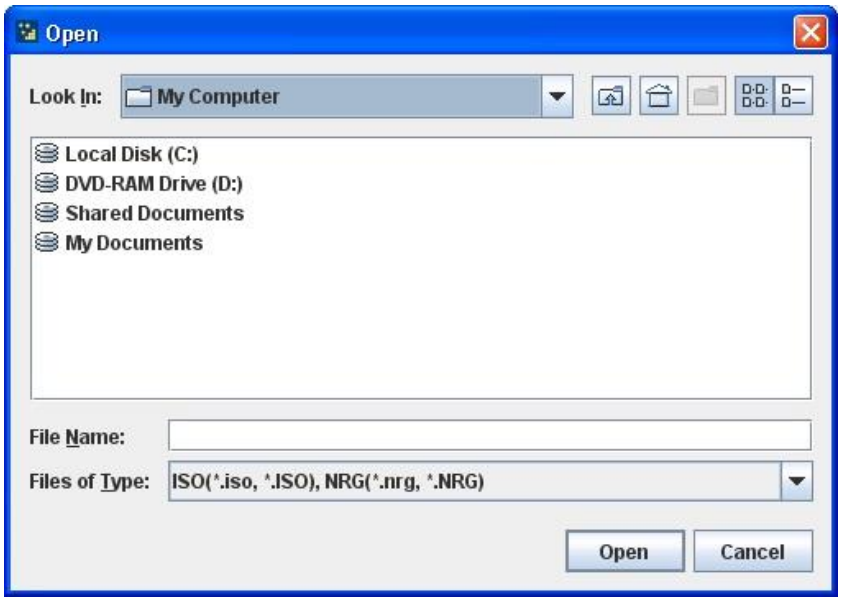
Item	Description
[Browse]	Add image file as virtual media.
[Connect]/[Disconnect]	Connect or disconnect selected device to the system.
[Close]	Closes this window.

Note

- If you replace media while connecting to virtual media, click [Disconnect] button after setting new media. Click [Connect] again.
- When the [Video Redirection] window closes, all devices are disconnected from the server. Also, the devices are removed from the list.
- If mounting the media selected by virtual media fails when connecting the media, click [Disconnect] button and click [Connect] button again.

Click the [Browse] button to display the image file selection window. From the storage devices on the PC, you can select those to be connected to the system.

FIGURE 1.21 Image file selection window



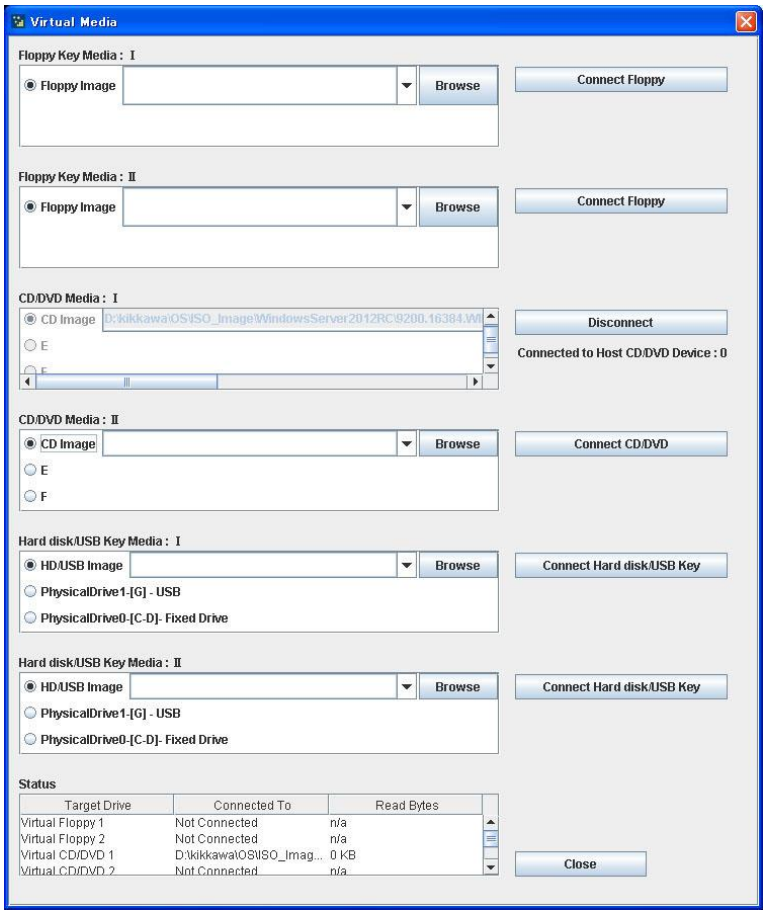
Items in image file selection window are listed below.

TABLE 1.12 Items in image file selection window

Item	Description
Look In	Displays the current search location
File name	Used to enter the device index letter (e.g., E:)
File of type	Used to specify a file type.
Open	Adds the selected device to the list.
Cancel	Closes this window.

Below formats of image can be used for virtual media.
Floppy: ima, img
CD/DVD: nrg, iso
HDD/USB: img
Select the ISO image file, and click the [Select] button. Then, the display returns to the [Virtual Media] window. Click [Connect CD/DVD] button in [Virtual Media] window to register the ISO image to target list of virtual media.

FIGURE 1.22 [Virtual Media] window (2)



CHAPTER 2 Component Configuration and Replacement (Add, Remove)

This section describes the configuration and replacement of component of the Cisco C880 server.

2.1 High availability configuration

This section describes the following functions for realizing a high system availability of the Cisco C880 server.

- 2.1.1 Memory Operation Mode
- 2.1.2 Memory Mirror
- 2.1.3 Hardware RAID

2.1.1 Memory Operation Mode

The Memory Operation Mode can be set from the MMB Web-UI. The following five modes are supported as Memory Operation Modes.

- Performance Mode
- Normal Mode
- Partial Mirror Mode
- Full Mirror Mode
- Spare Mode

The default is Normal Mode.
The overview of each mode is given the TABLE below.

TABLE 2.1 Overview of Memory Operation Modes

Memory Operation Mode	Description
Performance Mode	Mode that elicits the maximum memory performance. However, it does not support any RAS function except the SDDC.
Normal Mode	Mode in which the Memory Mirror and Memory Spare are used. DDDC is supported as a memory RAS function in addition to SDDC. Mode which is set as the default.
Full Mirror Mode	Mode in which the Memory Mirror is used in all the SBs included in the system. In this mode, mirror maintenance mode or the capacity maintenance mode is selected as the Memory Mirror RAS mode. For details on the Memory Mirror, see 2.1.2 Memory Mirror. For details on the Memory Mirror RAS, see Memory Mirror RAS of 2.1.2 Memory Mirror.
Partial Mirror Mode	The Memory Mirror mode is used only in the Home SB. In this mode, mirror maintenance mode or capacity maintenance mode is selected as the Memory Mirror RAS mode. For details on the Memory Mirror, see 2.1.2 Memory Mirror. For details on the Memory Mirror RAS, see Memory Mirror RAS of 2.1.2 Memory Mirror.
Spare Mode	Mode in which the Memory Spare is used. **Note** - The Memory Spare cannot be used if the Memory Mirror has been set. - In memory spare mode, the memory size recognized by the operating system decreases by from about two-thirds to five-sixth of memory size mounted physically in the system.

2.1.2 Memory Mirror

In the Cisco C880 server, the Mirror Mode and the Partial Mirror Mode are supported as the memory mirror, in which the function with the CPU is used. Full Mirror/Partial Mirror can be selected from the MMB Web-UI.

TABLE 2.2 Memory Mirror Mode

Mirror type	Description
Full Mirror	Memory Mirroring is executed to memories on all SBs included in a partition.
Partial Mirror	Memory Mirroring is executed to memories on only Home SB included in a partition. Memory Mirroring is not executed for an SB which is not the Home SB.

Memory Mirror RAS

This section describes the operation when there is an error in the DIMM in the Memory Mirror status.

- The Memory operation when using the Memory Mirror is selected from the MMB Web-UI.
- Mirror maintenance mode (the default)
  When restarting the system, the failed DIMM and the paired DIMM are not incorporated. The other normal DIMMs will maintain the Memory Mirror.
  - The Memory Mirror status will be maintained because only the normal DIMM would be used.
  - Since the DIMM area suspected to have failed will be degraded, the memory capacity seen from the operating system will be reduced.
- Memory capacity maintenance mode
  The Memory Mirror status of the memory mirror group in which the memory suspected to have failed will be deleted after the system is restarted. Up to six The DIMM (DIMM with the same NN number as the DIMM#NNM), including the failure suspected memory are not incorporated. The memory mirror group maintains the status of the Memory Mirror.

For details on the memory mirror group, see 'TABLE 2.3 Memory mirror group'.

TABLE 2.3 Memory mirror group

Memory mirror group 1	Memory mirror group 2	Memory mirror group 3	Memory mirror group 4
DIMM#0A0	DIMM#0C0	DIMM#1A0	DIMM#1C0
DIMM#0A1	DIMM#0C1	DIMM#1A1	DIMM#1C1
DIMM#0A2	DIMM#0C2	DIMM#1A2	DIMM#1C2
DIMM#0A3	DIMM#0C3	DIMM#1A3	DIMM#1C3
DIMM#0A4	DIMM#0C4	DIMM#1A4	DIMM#1C4
DIMM#0A5	DIMM#0C5	DIMM#1A5	DIMM#1C5
DIMM#0B0	DIMM#0D0	DIMM#1B0	DIMM#1D0
DIMM#0B1	DIMM#0D1	DIMM#1B1	DIMM#1D1
DIMM#0B2	DIMM#0D2	DIMM#1B2	DIMM#1D2
DIMM#0B3	DIMM#0D3	DIMM#1B3	DIMM#1D3
DIMM#0B4	DIMM#0D4	DIMM#1B4	DIMM#1D4
DIMM#0B5	DIMM#0D5	DIMM#1B5	DIMM#1D5

- Since the memory mirror group having a failure suspected DIMM operates in the Non Mirror, the status would be Partial Memory Mirror.
- Since half the number of DIMMs having a failure suspected DIMM in a Partial Mirrored memory group will not be incorporated, the memory capacity seen from the operating system will be maintained.

The memory incorporation status before and after the system restart is shown below.

FIGURE 2.1 Status when there is an error in the memory (mirror maintenance mode)

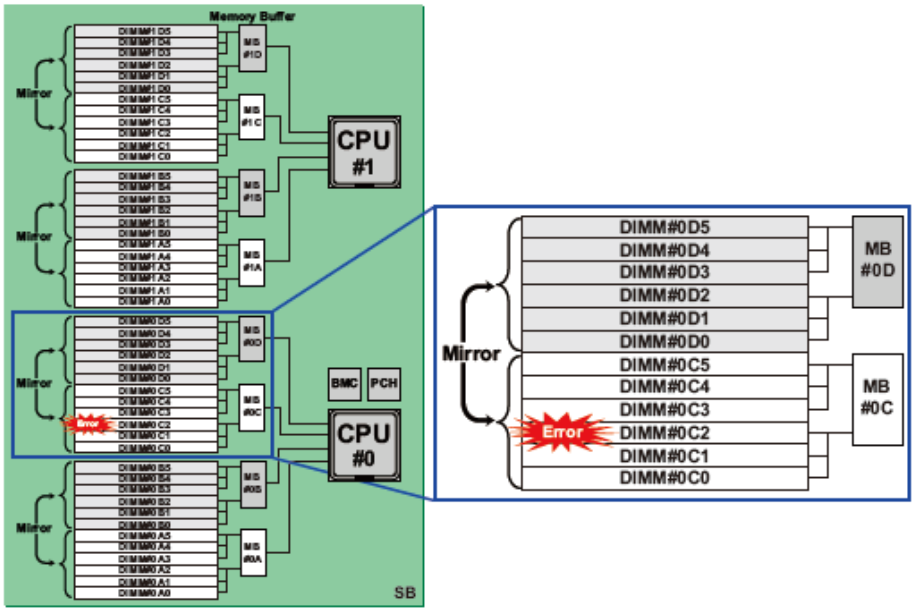


FIGURE 2.2 Status when the error had occurred in the system was restarted (mirror maintenance mode)

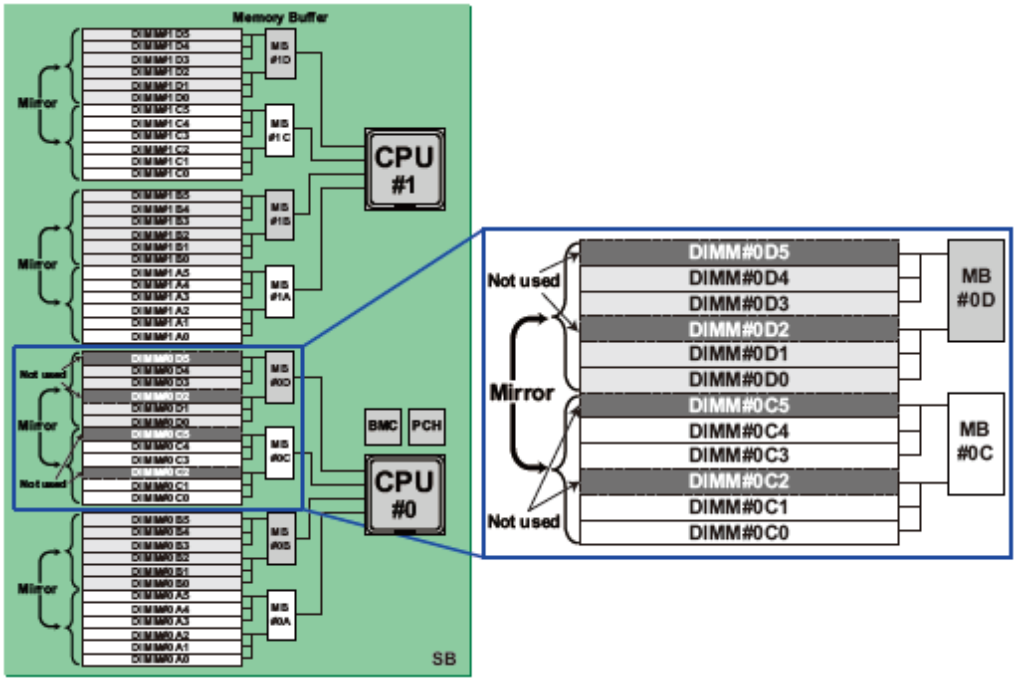


FIGURE 2.3 Status when there error has occurred in the memory (memory capacity maintenance mode)

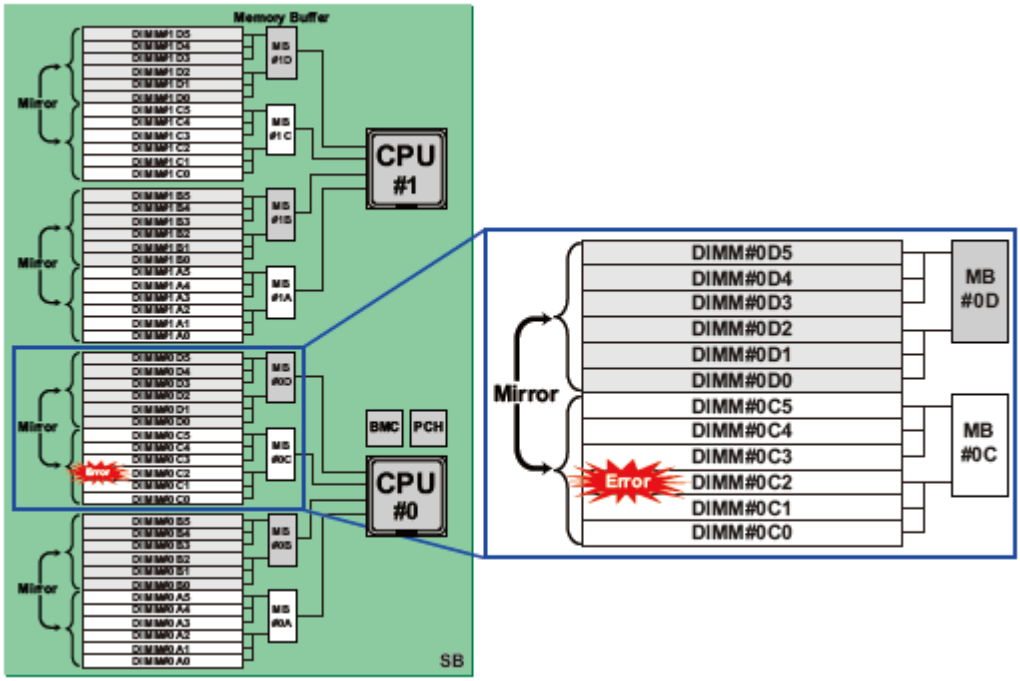
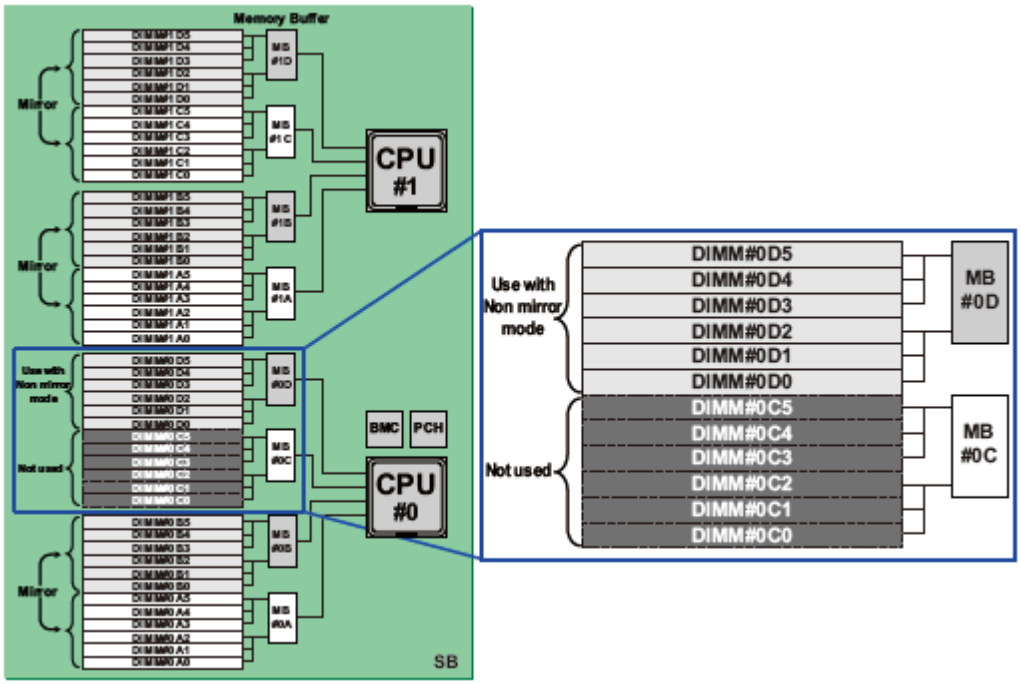


FIGURE 2.4 Status when an error has occurred in the memory (memory capacity maintenance mode)



The patterns supported in the combination of memory mirror status and failed DIMM are listed in the table below.

TABLE 2.4 Combination of the memory mirror status and the failed DIMM (Non Mirror)

Mirror RAS Mode	Mirror mode before reboot (during operation)	Places where the DIMM has failed	Mirror mode after reboot	Memory capacity after reboot
Mirror Keep Mode	Full Mirror	Mirror part	Full Mirror	Reduction
	Partial Mirror	Mirror part	Partial Mirror	Reduction
		Non Mirror part	Partial Mirror	Reduction

Mirror RAS Mode	Mirror mode before reboot (during operation)	Places where the DIMM has failed	Mirror mode after reboot	Memory capacity after reboot
Capacity Keep Mode	Full Mirror	Mirror part	Partial Mirror or Non-Mirror	No change
	Partial Mirror	Mirror part	Partial Mirror or Non-Mirror	No change
		Non Mirror part	Partial Mirror	Reduction

Memory Mirror conditions

The DIMM is mounted following the 'G.2.1 DIMM mounting sequence'.
The condition for the hardware is to have the same capacity as that of the mirroring DIMM group.

Memory Mirroring

Memory Mirroring is executed in the memory on the same SB.

2.1.3 Hardware RAID

The Cisco C880 server supports Hardware RAID.
Hardware RAID is a RAID function that performs operations using the SAS array controller card. The SAS array controller card is a PCI Express card having a dedicated RAID controller chip and firmware, and which can control the array (faulty HDD disconnection, incorporation, LED control).
RAID levels supported in the hardware RAID are RAID0, RAID1, RAID5, RAID6, RAID1E, RAID10, RAID50, and RAID60.
However, RAID level supported in the HDD/SSD on the SB and DU are RAID0, RAID1, RAID5, RAID6, RAID1E, and RAID10.
For details on the HDD/SSD replacement of the hardware RAID configuration, see '5.3 Replacing HDD/SSD when active replacement is not possible'.
Note

- The logical volume configured with hardware RAID except for RAID0 cannot be used by Software RAID.
- When using the hardware RAID, consider either of the following conditions to protect the customer's data in the event of a power failure.
- An FBU is mounted.
- Ensure stable AC power by redundant power mechanism, dual system reception mechanism, and UPS.

2.1.4 Cluster configuration

- For inter-cabinet clustering, clustering with only Cisco C880 server is supported. The inter-cabinet clustering with cabinets other than Cisco C880 server is not supported.

2.2 Replacing components

Components to be replaced can be identified from the replacement board and OPL LED display. For details on the LED display, see Appendix E Status Checks with LEDs.

2.2.1 Replaceable components

Replaceable components and replacement conditions are listed in the table below.

TABLE 2.5 Replaceable components and replacement conditions

Component name	AC power off (Device stop)	AC power on System off (hot maintenance)	AC power on System on (hot maintenance)
PSU_P/PSU_S	Replaceable	Replaceable	Replaceable (*1)
FANM	Replaceable	Replaceable	Replaceable (*1)
FANU	Replaceable	Replaceable	Replaceable
FANM	Replaceable	Replaceable	Replaceable
SB	Replaceable	Replaceable	Not replaceable

Component name		AC power off (Device stop)	AC power on System off (hot maintenance)	AC power on System on (hot maintenance)
	CPU	Replaceable	Replaceable	Not replaceable
	DIMM	Replaceable	Replaceable	Not replaceable
	Mezzanine	Replaceable	Replaceable	Not replaceable
	DIMM	Replaceable	Replaceable	Not replaceable
	Battery	Replaceable	Replaceable	Not replaceable
IOU_1GbE/IOU _10GbE		Replaceable	Replaceable	Not replaceable
	PCI Express card	Replaceable	Replaceable	Not replaceable
DU		Replaceable	Replaceable	Not replaceable
	PCI Express card	Replaceable	Replaceable	Not replaceable
	FBU	Replaceable	Replaceable	Not replaceable
	HDD/SSD	Replaceable	Replaceable	Replaceable (*2)
MMB		Replaceable	Not Replaceable	Not replaceable
OPL		Replaceable	Not replaceable	Not replaceable
MP, PDB		Replaceable	Not replaceable	Not replaceable

*1: Possible only in redundancy configuration.
*2: Possible only for redundancy configuration with RAID.

2.2.2 Component replacement conditions

This section describes the replacement conditions of each component.

PSU

The PSU unit can be replaced while the system continues operating. PSU replacement in a non-redundant configuration requires the system to be stopped.

FAN

The FAN unit can be replaced while the system continues operating.

SB

SB can be replaced when the system is powered off.
Remarks
Since the CPU/Mezzanine/DIMM which is mounted on the SB can be replaced after removing the SB from the device, the replacement can be done under the same conditions as the SB.
Note
Since there may be a time deviation after the Home SB is replaced, set the time in the operating system when the NTP is not used.

IOU_1GbE/IOU_10GbE

IOU_1GbE and IOU_10GbE can be replaced when the system is powered off.

DU

DU can be replaced when the system is powered off.

MMB

MMB can be replaced when AC power of the system is off.

2.2.3 Replacement procedures in cold maintenance

This section describes the procedures before and after replacement in cold maintenance.

Procedure before replacement

Stop the system.

Procedure after replacement

Start the system.

2.2.4 Replacing the battery backup unit of the uninterrupted power supply unit (UPS)

This section describes the procedure for replacing the battery backup unit of the UPS. The UPS battery is regularly replaced and the life cycle is monitored by the standard monitoring function of the operating system.

2.2.5 Replacing the PCI SSD card

This section describes the procedure for replacing the PCI SSD card.
Note
The PCI SSD card does not support hot replacement. Stop the system before replacing.

In a RAID configuration (Linux software RAID)

1. Place the faulty PCI Express card offline and remove the card.
   Example:

```
# mdadm/dev/md0 –fail  /dev/fiob
# mdadm/dev/md0–remove  /dev/fiob
```

2. Power off the system.
3. Replace the faulty PCI Express card.
4. Power on the system.
5. Initialize the replaced PCI Express card.
6. The executing procedure is as follows.
   a. fio-detach (Disconnecting the device from the operating system)
   b. fio-format (Low level formatting of the device)
   c. fio-attach ((Making the device available on the operating system)

      Example:

```
# fio-detach /dev/fct1
# fio-format /dev/fct1
# fio-attach /dev/fct1
```

   Remarks
   The work of adding the device will trigger the rebuild operation.
   Example:

```
# mdadm /dev/md0 –add /dev/fiob
```

In SWAP configuration

1. Delete the swap entry of the faulty PCI Express card.

```
(Example) # swapoff /dev/fioal
```

2. Confirm the serial number of the faulty PCI card
3. Delete the serial number of the failed PCI card from the pre-allocate memory in /etc/modprobe.d/ioMemory-vsl.conf.
   Note
   Before replacing the PCI card, delete the serial number of the faulty PCI card from the pre-allocate memory in /etc/modprobe.d/ioMemory-vsl.conf.
4. Power off the system.
5. Replace the faulty PCI Express card.
6. Power on the system.
7. Initialize the replaced PCI Express card.
   The executing procedure is as follows.
   a fio-detach (Disconnecting the device from the operating system)

b fio-format (Low-level formatting of the device)

Remarks
If the device is used as a SWAP device, the formatting must have a 4K sector size.

c fio-attach (Making the device available on the operating system)
Example:

```
# fio-detach /dev/fct0
# fio-format –b 4K /dev/fct0
# fio-attach /dev/fct0
```

8. Create a swap entry for the replaced PCI Express card.
Remarks
A system must be created before creating a swap entry.
Example:

```
# mkswap /dev/fioa1
# swapon /dev/fioa1
```

9. Confirm the serial number of the replaced PCI Express card.
10. Register the serial number of the replaced PCI Express card in the pre-allocate memory in /etc/modprobe.d/ioMemory-vsl.conf.
Note
After replacing the PCI Express card, add the target serial number in the pre-allocate memory in /etc/modprobe.d/ioMemory-vsl.conf.
11. Restart the system (operating system).

2.3 Expansion of components

This section describes how to add components.
The components and the conditions for maintaining the addition of each component are listed in the table below.
Some components cannot be added.

TABLE 2.6 Expandable components

Component name			AC power off (Device stop)	AC power on System off (hot maintenance)	AC power on System on (hot maintenance)
PSU_P/PSU_S			Expandable	Not Expandable	Not Expandable
	FANM		-	-	-
FANU			-	-	-
	FANM		-	-	-
SB			Expandable	Expandable	Not expandable
	CPU		Expandable	Expandable	Not expandable
	DIMM		Expandable	Expandable	Not expandable
	Mezzanine		-	-	-
		DIMM	Expandable	Expandable	Not expandable
	battery		-	-	-
IOU_1GbE/IOU_10GbE			Expandable	Expandable	Not expandable
	PCI Express card		Expandable	Expandable	Not expandable
DU			Expandable	Expandable	Not expandable
	PCI Express card		Expandable	Expandable	Not expandable
	FBU		-	-	-
	HDD/SSD		Expandable	Expandable	Expandable
MMB			Expandable	Expandable	Expandable
OPL			-	-	-
MP, PDB			-	-	-

- : Outside the expansion target

Perform the license authentication following the Windows window instructions.

Windows license authentication

1. When starting Windows, click the balloon for license authentication that is displayed in the task tray.
2. Click [Product Key Input] and enter the product key found on the COA label attached to rear lateral side of the cabinet.
3. License authentication can be performed via the Internet or by making a phone call to the Microsoft customer service center.

Hot add procedure for HDD/SSD

For details on the hot add procedure for HDD/SSD, see CHAPTER 3 Replacement of HDD/SSD.

Changing the firmware when expanding components

The firmware may be required to be changed when expanding a component.
Use the same firmware version number of the FC (Fiber Channel) card within the system.

- FC card (PCI Express card)
  Use the same version number as the firmware version number that is currently in use.

CHAPTER 3 Replacement of HDD/SSD

This chapter describes how to replace Hard Disk Drives (HDD) or Solid State Drives (SSD).
In Cisco C880 M4 server (E7-8800 v3 CPU), it is required to use HII Configuration Utility for replacing a HDD or SSD.
In Cisco C880 M4 server (E7-8800 v2 CPU), it is required to use WebBIOS for replacing a HDD or SSD.

3.1 Hot replacement of HDD/SSD with Hardware RAID configuration

This section describes how to replace Hard Disk Drives (HDD) or Solid State Drives (SSD) with Hardware RAID configuration.

3.1.1 Hot replacement of failed HDD/SSD with RAID0 configuration

This section describes the workflow of hot replacement of HDD or SSD with RAID0 configuration when one HDD or SSD fails.
Remarks

- Hot replacement of HDD or SSD can be performed only when HDDs or SSDs are mirror configuration by using software.
- Step1 and Step2 are performed by field engineers in charge of your system.

1. Replace HDD or SSD with the Alarm LED on by using MMB Maintenance Wizard.
2. Create a logical drive with RAID0 configuration by using MMB Maintenance Wizard.
3. Confirm whether [Status] of replaced HDD or SSD has been already ‘Operational’ by MMB Web-UI. How to confirm the status differs depending on whether the HDD or SSD is included or in a DU.

3.1.2 Hot replacement of failed HDD/SSD with RAID 1, RAID 1E, RAID 5, RAID 6, or RAID 10 configuration

This section describes the workflow of hot replacement of HDD or SSD with RAID 1, RAID 1E, RAID 5, RAID 6, or RAID 10 configuration when one HDD or SSD fails.
Remarks

- Step1 is performed by field engineers in charge of your system.
- Copy back may run after rebuild has been completed.

1. Replace the HDD or SSD with the Alarm LED on by using MMB Maintenance Wizard.
   Note
   When set a spare disk, set the HDD or SSD to the spare disk by using Maintenance Wizard if the status of the replaced HDD or SSD is ‘Available’.
2. Confirm whether a rebuild of the HDD or SSD has been already completed by using the below steps depending on whether a spare disk is set or not.
   - If not set a spare disk
     A rebuild is automatically performed to replaced HDD or SSD. Then, the Alarm LED of the HDD or SSD starts blinking.
     Confirm whether a rebuild of replaced HDD or SSD has been already completed by MMB Web-UI. How to confirm the status differs depending on whether the HDD or SSD is included in a DU.
   - If set a spare disk:
     A rebuild has been already automatically performed to the HDD or SSD set as a spare disk. The replaced HDD or SSD automatically becomes a spare disk. The Alarm LED of the HDD or SSD goes out.
     Confirm whether [Status] of replaced HDD or SSD has been already ‘Hot spare’ by MMB Web-UI. How to confirm the status differs depending on whether the HDD or SSD is included in a DU.

3.2 Preventive replacement of HDD/SSD with Hardware RAID configuration

This section describes how to perform the preventive replacement of Hard Disk Drives (HDD) or Solid State Drives (SSD) with Hardware RAID configuration.

3.2.1 Preventive replacement of failed HDD/SSD with RAID0 configuration

This section describes the workflow of preventive replacement of HDD or SSD with RAID0 configuration.

For mirror configuration

Hot preventive replacement can be performed if HDDs or SSDs are mirror configuration by software.
Remarks

- Step1 and Step2 are performed by field engineers in charge of your system.
- If HDD or SSD other than target HDD or SSD for preventive replacement fails in step3, field engineers in charge of your system replace the failed HDD or SSD.

1. Replace HDD or SSD with the Alarm LED on by using MMB Maintenance Wizard.
2. Create a logical drive with RAID0 configuration by using MMB Maintenance Wizard.
3. Confirm whether [Status] of replaced HDD or SSD has been already ‘Operational’ by MMB Web-UI. How to confirm the status differs depending on whether the HDD or SSD is included in a DU.

For non-mirror configuration (replacement with the system power off)

If HDDs or SSDs are not mirror configuration, preventive replacement of a HDD or SSD has to be performed with the system power off
Remarks

- If HDD or SSD other than target HDD or SSD for preventive replacement fails in step3, field engineers in charge of your system replace the failed HDD or SSD.
- Step7 is performed by the field engineer in charge of your system.

1. Back up data in all HDDs or SSDs connected to the RAID controller card to which the target HDD or SSD for preventive replacement is connected.
2. Confirm the HDD or SSD which S.M.A.R.T. has predicted to fail by MMB Web-UI checking mounting location. How to confirm the status differs depending on whether the HDD or SSD is included in a DU.
3. If HDD or SSD other than target HDD or SSD for preventive replacement fails, replace the failed HDD or SSD prior to perform preventive replacement
4. Restart the system.
   In C880 M4 server (E7-8800 v3 CPU), start HII Configuration Utility from Boot Manager front page.
   In C880 M4 server (E7-8800 v2 CPU), Start WebBIOS from Boot Manager front page.
5. In C880 M4 server (E7-8800 v3 CPU), Perform Clear Configuration.
   Selet [Clear Configuration] from [Configuration Utility] in [HII Configuration Utility].
   Note
   If you perform [Clear Configuration], all data are deleted.

   In C880 M4 server (E7-8800 v2 CPU), Perform Clear Configuration or delete a VD.

   - For there is only one VD with RAID 0:
     - Select [Clear Configuration] from [Configuration Wizard] in [WebBIOS] and click [Next].
     - If below massage appears, click [Yes].
       “This is Destructive Operation.
       Original configuration and data will be lost.
       Select Yes, if desired so.”
       Note
       If you perform [Clear Configuration], all data are deleted. [Configuration Preview] window appears.

- For the VD number of RAID 0 group is the most biggest among the environment where there are multiple VDs:
  Select the particular VD and delete it.

6. When the data has been erased, exit WebBIOS and power off the system.
7. Replace the HDD or SSD which S.M.A.R.T. predicted to fail.
8. Start the system.
   In C880 M4 server (E7-8800 v3 CPU), start HII Configuration Utility from the Boot Manager front page.
   In C880 M4 server (E7-8800 v2 CPU), start WebBIOS from the Boot Manager front page.
9. Create an array configuration.
   In C880 M4 server (E7-8800 v3 CPU), create an array configuration with HII Configuration Utility.
   In C880 M4 server (E7-8800 v2 CPU), create an array configuration with WebBIOS.
10. Restore backup data or reinstall the operating system.

3.2.2 Preventive replacement of failed HDD/SSD with RAID 1, RAID 1E, RAID 5, RAID 6, or RAID 10 configuration

This section describes the workflow of preventive replacement of HDD or SSD with RAID 1, RAID 1E, RAID 5, RAID 6, or RAID 10 configuration.

Remarks

From step1 to step6 are performed by the field engineer in charge of your system.

1. Make data consistent by MMB Maintenance Wizard to make the HDD or SSD no error.
2. Turn on Alarm LED of the HDD or SSD which S.M.A.R.T. predicted to fail by MMB Maintenance Wizard.
3. Confirm the location of the HDD or SSD, tuning off the Alarm LED by MMB Maintenance Wizard.
4. Make the target HDD or SSD offline by MMB Maintenance Wizard
5. Confirm that [Status] of the target HDD or SSD is ‘Failed’ or ‘Available’.
6. Replace the HDD or SSD of which you confirmed in step2 that Alarm LED turns on.
   Note
   When set a spare disk, set the HDD or SSD to the spare disk by using Maintenance Wizard if the status of the replaced HDD or SSD is ‘Available’.
7. Confirm whether a rebuild of the HDD or SSD has been already completed by using the below steps depending on whether a spare disk is set or not.

   - If not set a spare disk
     A rebuild is automatically performed to replaced HDD or SSD. Then, the Alarm LED of the HDD or SSD starts blinking.
     Confirm whether a rebuild of replaced HDD or SSD has been already completed by MMB Web-UI. How to confirm the status differs depending on whether the HDD or SSD is included in a DU.

     - For replacement of a HDD or SSD included in a DU
       Confirm whether [Status] of replaced HDD or SSD has been already ‘Operational’ by [System] – [DU] – [DUx] window of MMB Web-UI.

   - If set a spare disk:
     A rebuild has been already automatically performed to the HDD or SSD set as a spare disk. The replaced HDD or SSD automatically becomes a spare disk. The Alarm LED of the HDD or SSD goes out.
     Confirm whether [Status] of replaced HDD or SSD has been already ‘Hot spare’ by MMB Web-UI. How to confirm the status differs depending on whether the HDD or SSD is included in a DU.

     - For replacement of a HDD or SSD included in a DU
       Confirm whether [Status] of replaced HDD or SSD has been already ‘Hot Spare’ by [System] – [DU] – [DUx] window of MMB Web-UI.

3.3 Replacement of HDD/SSD in case hot replacement cannot be performed

In below cases, hot replacement of the failed HDD or SSD cannot be performed.

- Case where multiple deadlock occurs
  Multiple deadlock occurs when more than one hard disk fail to be recognized at the same time.
- The HDD or SSD is RAID0 configuration and it is not mirror configuration by software.
  If a HDD or SSD fails in this case, it is required to reconfigure the Hardware RAID after replacing HDD or SSD. Recover from back up data because data in failed HDD or SSD is not guaranteed.

When replacing the HDD or SSD, it has to be done with the system power off. The workflow is described below.

Remarks

Step2 is performed by the field engineer in charge of your system.

1. Turn off the power to the system.
2. Replace the HDD or SSD.
3. Restart the system
   In C880 M4 server (E7-8800 v3 CPU), start HII Confguration Utility from Boot Manager front page.
   In C880 M4 server (E7-8800 v2 CPU), start WebBIOS from the Boot Manager front page.
4. Create the array configuration
   In C880 M4 server (E7-8800 v3 CPU), create the array configuration with HII Configuration Utility.
   In C880 M4 server (E7-8800 v2 CPU), create the array configuration with WebBIOS.
5. Restore the data for backup.

CHAPTER 4 Backup and Restore

This chapter describes the backup and the restore operations required for restoring server data.

4.1 Backing Up and Restoring Configuration Information

The MMB has BIOS configuration information for the system. It also has backup and restore functions for the configuration information on the MMB.

Notes

- Configuration information on the server must be backed up ahead of time. The backup enables restoration of the original information if the system becomes damaged or an operational error erases data on the server. Be sure to periodically backup server configuration information in case of such events.
- The Cisco C880 server cannot be connected to an FDD (floppy disk) for backup, restore, or other such operations. To use an FDD, connect it to a remote PC or another server connected to the Cisco C880 server.

This section describes the backup and the restore operations for UEFI configuration information and MMB configuration information.

4.1.1 Backing up and restoring UEFI configuration information

Users can perform the following processes with the backup and restore functions for UEFI configuration information:

- After setting UEFI configuration, backing up setting UEFI configuration.
- Restoring backed-up UEFI configuration information during replacement of a faulty SB

A remote terminal can store the saved information. The data saved to the remote terminal can be restored. In the [Backup BIOS Configuration] window of the MMB Web-UI, back up UEFI configuration information to the PC running your browser. The procedure is as follows.

Backing up UEFI configuration information

1. Click the [Backup] button.
   The save destination dialog box of the browser appears.
2. Select the save destination path. Then, click the [OK] button.
   Download of the file begins.
   The default BIOS Configuration file name for the backup is as follows:
   BIOS_save date_BIOS version.dat

Restoring UEFI configuration information

From the [Restore BIOS Configuration] window, restore BIOS configuration information.

1. Select the backup BIOS Configuration file stored on the remote PC. Then, click the [Upload] button.
   File transfer to the MMB begins.
   The following window appears when the file transfer is completed.
2. Click the [Restore] button.

4.1.2 Backing up and restoring MMB configuration information

From the Backup/Restore MMB Configuration window, you can back up and restore MMB configuration information. The procedure is as follows.

Backing up MMB configuration information

1. Click the [Backup] button.
   The browser dialog box for selecting the save destination appears.

2. Select the save destination path. Then, click the [OK] button.
   Download of the file begins. The default MMB Configuration file name for the backup is as follows:
   MMB_(*save date*)_(*MMB version*).dat

Restoring MMB configuration information

1. Confirm that the system has stopped completely.
2. Select the backup MMB Configuration file stored on the Remote PC. Then, click the [Restore] button.
   File transfer to the MMB begins. A restore confirmation dialog box appears when the file transfer is completed.

FIGURE 4.1 Restore confirmation dialog box

3. To restore MMB configuration information, click the [OK] button. To cancel restoration, click the [Cancel] button.

CHAPTER 5 Chapter System Startup/Shutdown and Power Control

This section describes the startup, shutdown and the power control in Cisco C880 server.

5.1 System Power on and Power off

This section describes various procedures of power on and Power off for the system and explains the method of checking power supply.

5.1.1 Various Methods for Powering On the System

There are three methods for powering on the system, which are as follows.

1. Operation through the MMB Web-UI or MMB CLI.
   The system can be powered on through the MMB Web-UI or MMB CLI operation.
2. Scheduled operation (Automatic operation according to a set schedule)
   A system can be powered on by a scheduled operation (Automatic operation function).
3. Wake On LAN (WOL)
   The system can be power on with WOL.

Notes

- You can enable or disable WOL of LAN ports on IOU per IOU by MMB Web-UI. Default value of WOL is 'disable'. If you use WOL of LAN port on IOU, set Onboard LAN Mode to 'Enabled' (WOL enable).
- If the power supply is stopped or IOU is pulled out, the setting of WOL is initialized.
  Restore the setting of WOL with Operating System.
- Enable or Disable WOL is set from both BIOS and the operating system.
  To enable WOL in Windows, following settings are required for each port of the device manager Check the [Wake On Magic Packet from the powered off state] checkbox in [Device Manager] – [Network Adaptor] – [INTEL ® 82576 Gigabit Dual Port Network Connection] – [Property] – [Power Management].
  In case of setting in windows, "Intel PROSet" of the supplied driver must be installed.
  To enable WOL in BIOS, following setting is required for each port:
  Enable [Wake on LAN] in the menu [Device Manager]-[Network Device List]-[NIC Configuration]

5.1.2 Types of Power off Method of System

The three methods to power off the system are as follows.

1. Shutdown from the operating system (Recommended)
   Shutdown the operating system by using the operating system commands. When powering off the system, perform the shutdown from the operating system. For the operating system shutdown commands, refer to the manual of each operating system.
2. Powering off of the system using the [MMB Web-UI] window or the MMB CLI.
   The power can be turned off by the Web window operation of an external terminal, or the MMB CLI.
3. Powering off the system by a scheduled operation.
   The system can be powered off by a scheduled operation (Automatic operation function).

Notes
In the following cases, confirm the details according to '6.2 Troubleshooting'. If the error recurs, contact your sales representative or field engineer.
Before contacting, confirm the model name and serial number shown on the label affixed on the main unit.
Until the problem is solved, do not execute [Reset], [Force Power Off] for the system.

- When [Power Off], [Reset], or [Force Power Off] is executed for system, or when shutting down from the operating system, the MMB Web-UI (Information area) status changes to "Error".

- When the MMB Web-UI displays the status of each component, “Read Error” will be displayed in the Part number and Serial number.

5.1.3 Procedure for System Power On and Power Off

The privileges for powering on and powering off the system are as follows.

TABLE 5.1 Privilege for power on and power off

User Privilege	Power on and power off privilege
Administrator	Has permission.
Operator	Has permission
User	Does not have permission
CE	Does not have permission

5.1.4 System Power on by MMB

This section describes the procedure of powering on the system by MMB.

1. Log into the MMB Web-UI.
   -> [MMB Web-UI] window appears.
2. Click [System] – [Power Control].
   -> [Power Control] window appears.
3. Click the [Apply] button.
   -> A confirmation dialog box appears.
4. Click the [OK] button to execute, and click the [Cancel] button to cancel.

Remarks
A warning message appears if the system is already powered on, or if the specified control fails because the power is turned off.

5.1.5 Checking the System Power status by using the MMB

This section describes the procedure by which power status of system is confirmed.

1. Log in MMB Web-UI.
   -> The MMB Web-UI window appears.
2. Click [System] – [System Information].
   -> [System Information] window appears.

5.1.6 Powering off the system by using the MMB

This section describes the powering off procedure using the [MMB Web-UI] window.

1. Log into the MMB Web-UI.
   -> The MMB Web-UI window appears.
2. Click [System] – [Power Control] from the menu of the Web-UI.
   -> The [Power Control] window appears
3. Click the [Apply] button.
   -> The system will be powered off.

5.2 Scheduled operations

This section describes scheduled operations.

5.2.1 Powering on the system by scheduled operation

When a scheduled operation is set for the system, power is turned on, at the set time.

Daily, weekly, monthly, specific date or a combination of these options can be set as a schedule.
Note
The times recorded in the SEL may lag behind the scheduled operation as can be seen below.

- After the configuration check and preparation for the startup has been carried out, the power is turned on. It takes a while to start. In such case, the display of the SEL may be delayed by six to eight seconds, from the scheduled operation time.
- Shutdown instruction from the MMB to the operating system is executed within few seconds from the set time. However, the time shown below may change under various conditions, like setting, configuration, etc.
  - Time till the instruction reaches the operating system from the MMB
  - Time until the operating system shutdown is started and time until the start of the operating system shutdown is notified to the MMB
- Even if the [Power on Delay] is set to 0 seconds, it may take 30 ~ 70 seconds from the time of turning on the power and starting, up to reset.

5.2.2 Power off the system by scheduled operation

When a scheduled operation is set for the system, power is turned off at the set time.
A daily, weekly, monthly, specific date or a combination of these options can be set a schedule.

5.2.3 Relation of scheduled operation and power restoration function

In the Cisco C880 server, scheduled operation and power restoration function are linked when power restoration mode is set to “Schedule Sync”.

TABLE 5.2 Relationship between scheduled operation and system power restoration mode

No.	When there is power failure	When the power is restored	Always OFF (*1)	Always ON (*1)	Restore (*1)	Schedule Sync (*1)
1	Outside the operation time	Within the operation time	OFF	ON	OFF	ON
2	Within the operation time	Within the operation time	OFF	ON	ON	ON
3	Outside the operation time	Outside the operation time	OFF	ON	OFF	OFF
4	Within the operation time	Outside the operation time	OFF	ON	ON	OFF

ON: System Power On, OFF: System Power Off
Notes
Operations indicated by (*1) in the table, assume normal shutdown when a power failure occurs. If there is an abnormal power off because the UPS had not been used, the system will not automatically start (= OFF mode operation) in a restoration operation, irrespective of the operation settings.

5.2.4 Scheduled operation support conditions

The description of power on/off items, scheduled operation support conditions and menu items are listed in the table below.

TABLE 5.3 Power on/off

Menu Item	Scheduled operations	Description
Power On	Supported	Powers on the system.
Power Off	Supported	Powers off the system following an operating system shutdown.
Force Power Off	Not supported	Forcibly powers off the system without an operating system shutdown. This is used, to forcibly power off the system, when the shutdown from the operating system is disabled.

Menu Item	Scheduled operations	Description
Power Cycle	Not supported	Powers off and then powers on the system. The system is forcibly powered off without an operating system shutdown.
Reset	Not supported	Resets the system. This reset is not followed by a reboot of the operating system.
NMI	Not supported	Issues an NMI interrupt for the system.

5.3 Automatic System Restart Conditions

This section describes the setting of conditions to execute automatic system restart.

5.3.1 Setting automatic system restart conditions

Users with Administrators/Operator privilege can set system.
Note

- If you perform following operations, disable 'Boot Watchdog'..
  - Installation of operating system
  - Starting in the single user mode

When the above mentioned operations are executed with the Boot Watchdog in the [Enable] status, the specified action (Stop rebooting and Power Off or Stop rebooting or Diagnostic Interrupt assert) will be executed after repeating the operating system restart for specified number of times. The number of retries to restart the operating System and the actions to be executed depend on the settings in the [ASR (Automatic Server Restart) Control] window of the MMB.
At that time, Boot Watchdog can be forcibly set to [Disable] by checking the check box of [Cancel Boot Watchdog] and clicking the Apply button in the [ASR (Automatic Server Restart) Control] window.

The procedure of automatic restart condition setting of the system is as follows.

1. Click [System] – [ASR Control].
   -> The [ASR Control] window appears.
2. Set the automatic restart conditions.
   The setting items of the [ASR Control] window are listed in the table below.

TABLE 5.4 [ASR Control] window display / setting items

Items	Description
ASR	
Number of Restart Tries	Set the number of retries for restarting the operating system when the hardware error occurs and OS shuts down. The number of times can be set up to 0-10 times. When 0 is specified, it does not retry. Default is five times.
Action after exceeding Restart tries	Repeat the restart by Watchdog Timeout and sets the action when the above-mentioned retry number is exceeded. The actions are as below. - Stop rebooting and Power Off: Reboot process is stopped, power supply of system is cut off. - Stop rebooting: Reboot process is stopped, and the system is stopped. - Diagnostic Interrupt assert: Reboot process is stopped, instructs the NMI interruption for system. Tries to collect the data for investigation (damp) for the investigating the cause of stoppage, of the system which has stopped. Default setting is 'Stop rebooting and Power Off'
Retry Counter	Displays the number of actual possible retries.

Note
Must not set 'Boot Watchdog' and 'Software Watchdog' to "Enable".

5.4 Power Restoration

In the Cisco C880 server, the system operations for power restoration can be set in the chassis unit.

This can be set by MMB Web-UI.

5.4.1 Settings for Power Restoration

When using a UPS, the following items can be set when a power failure is detected. The default is “Restore”.

TABLE 5.5 Power Restoration Policy

Item	System operation
Always Off	Continues the power off status after the power is restored.
Always On	Power on the system after restoring the power irrespective of the status of the power failure.
Restore	Returns to the state at the time when the power failure occurred. Powers on the system that were On when the power failure occurred, and retains the power off status for system that were powered off when the power failure occurred.
Schedule Sync	Automatically powers on the system, according to the scheduled operation settings when a power failure had occurred during working hours. (*1)

*1: For details on the scheduled operations, see ‘5.2 Scheduled operations’.

If the startup of an external SAN unit connected to the UPS and such unit is slow during power restoration, then the SAN device does not become usable if the system is powered on by the server. Therefore, SAN boot may fail. In that case, “System Power On Delay” (units of seconds: 0 to 9999 seconds, default = 0 seconds) can be set in addition to the above mentioned settings.

5.5 Remote shutdown (Windows)

Windows with versions of Windows XP onwards, comes with a ‘shutdown.exe’ command. This command can be used for remote shutdown from a management terminal.

5.5.1 Prerequisites for remote shutdown

The following are the prerequisites for using the remote shutdown (Windows).

- The operating system of the management terminal should be one of the following.
  - Windows 8.1
  - Windows 8
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows 7
  - Windows Server 2008 R2
  - Windows Server 2008
  - Windows Server 2003 R2
  - Windows Server 2003 –Windows Vista
  - Windows XP
- The management terminal to be shutdown should be connected to Windows through a network.
- Firewall settings of the target Windows
  In the [Exception] settings of the firewall, [File and Printer Sharing] check box must be checked.
- When target is work group environment
  The user name and password of the management terminal must match those of the target Windows to be shut down.
- When the target is an Active Directory environment
  A user with administrative privileges for the Windows to be shut down must log in to the management terminal.

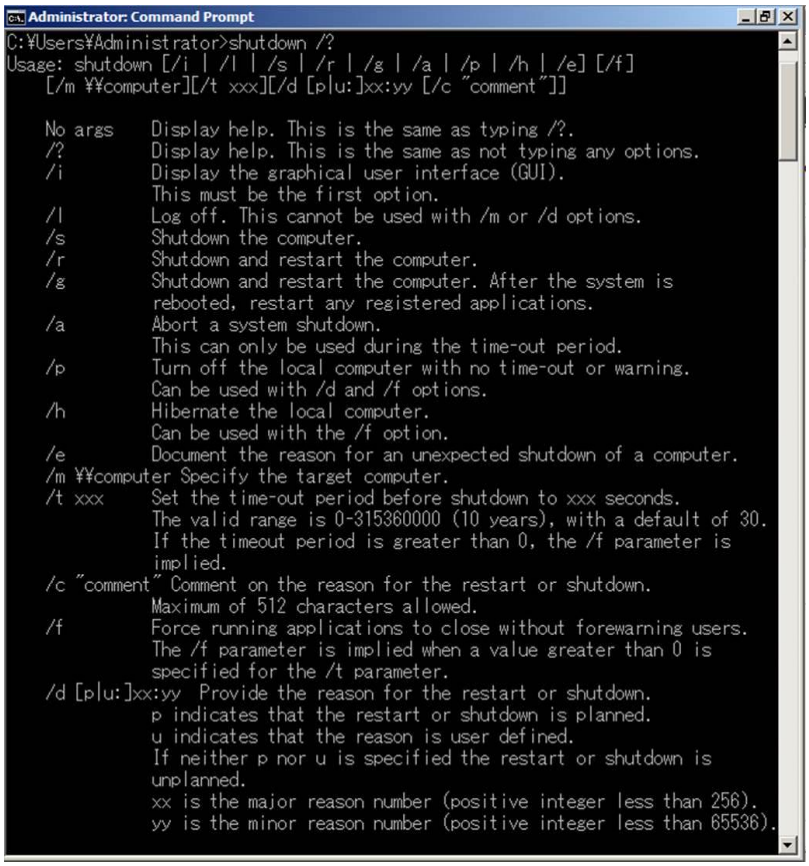
5.5.2 How to use remote shutdown

To perform remote shutdown, log in to the management terminal and enter the shutdown command.

```
Shutdown –s –m ¥¥ <Server Name>
```

In <Server Name>, specify the computer name of the Windows to be shut down.
For details on other options of the shutdown command, see 'Help'.
When the shutdown command is executed by using /? Option displays a simplified help.

Figure 5.1 Simplified help for the shutdown command



CHAPTER 6 Error Notification and Maintenance (Contents, Methods, and Procedures)

This chapter describes the maintenance functions provided by the Cisco C880 server. It also describes the actions to take for any problems that occur.

6.1 Maintenance

The Cisco C880 server supports hot maintenance of PSUs, fans and HDD/SSDs. This enables maintenance of the system as it continues operating.
For details and a list of the replaceable components, see 'CHAPTER 2 Component Configuration and Replacement (Add, Remove)'.
Remarks
Field engineers perform the maintenance on the Cisco C880 server.

6.1.1 Maintenance using the MMB

The MMB provides system maintenance functions through the [Maintenance] menu of the Web-UI.
You can use the [Maintenance] menu to back up and restore system configuration information.

6.1.2 Maintenance method

Maintenance is performed with the Maintenance Wizard on the MMB Web-UI from a terminal such as a PC connected to the MMB in the Cisco C880 server.
The MMB provides a dedicated Maintenance LAN port for field engineers. To perform maintenance using the Maintenance Wizard, a field engineer connects an FST (PC used by the field engineer) to the Maintenance LAN port of the MMB of the maintenance target system.
Note
Field engineers perform the maintenance on the Cisco C880 server.
Below settings are required for maintenance by the field engineers.

- Video redirection and virtual media are available.
- Telnet or SSH is available.

6.1.3 Maintenance modes

The Cisco C880 server has several maintenance modes.
Only field engineers are allowed to execute operations related to power control such as power off and power on in maintenance mode which can prevent error during this operations. The maintenance modes provide the following advantages:

- They prevent someone other than the field engineer from executing operations related to power control so that the system does not change to unexpected status.
- They prevent error reporting caused by a maintenance error (or maintenance work).

The following table lists the maintenance modes and their functions. Note that Operation mode is the normal operation mode and not a maintenance mode.

TABLE 6.1 Maintenance modes

Mode	Meaning
Operation [Normal operation]	Normal operation
Hot System Maintenance [Active for work (system)]	For maintenance work performed while the system power is on

Mode	Meaning
Cold System Maintenance (breaker on) [Stopped for work (standby)]	For maintenance work performed while the system power is off and the AC power supply is on
Cold System Maintenance (breaker off) [Stopped for work (AC off)]	For maintenance work performed while the system power is off and the AC power supply is off

TABLE 6.2 Maintenance mode functions

Item		Operation mode	Maintenance mode		
			Hot System	Cold System (breaker on)	Cold System (breaker off)
Power supply operation	Administrator	Permitted	Permitted	Suppressed	Suppressed
	Field engineer	Suppressed	Suppressed	Permitted	Permitted
Wake On LAN (WOL)		Permitted	Permitted	Suppressed	Suppressed
Calendar function		Permitted	Permitted	Suppressed	Suppressed
OS boot		Permitted	Permitted	Suppressed Stops at BIOS	Suppressed Stops at BIOS

6.1.4 Maintenance of the MMB

If the server with single MMB fails in MMB, take actions below.

1. Shut down the operating system (LAN) from a remote terminal. (*1)
2. Turn off the chassis AC power.
3. Replace the MMB.
4. Turn on the chassis AC power.

(*1) If you use only port of MMB to login the operating system, you cannot login to the operating system.

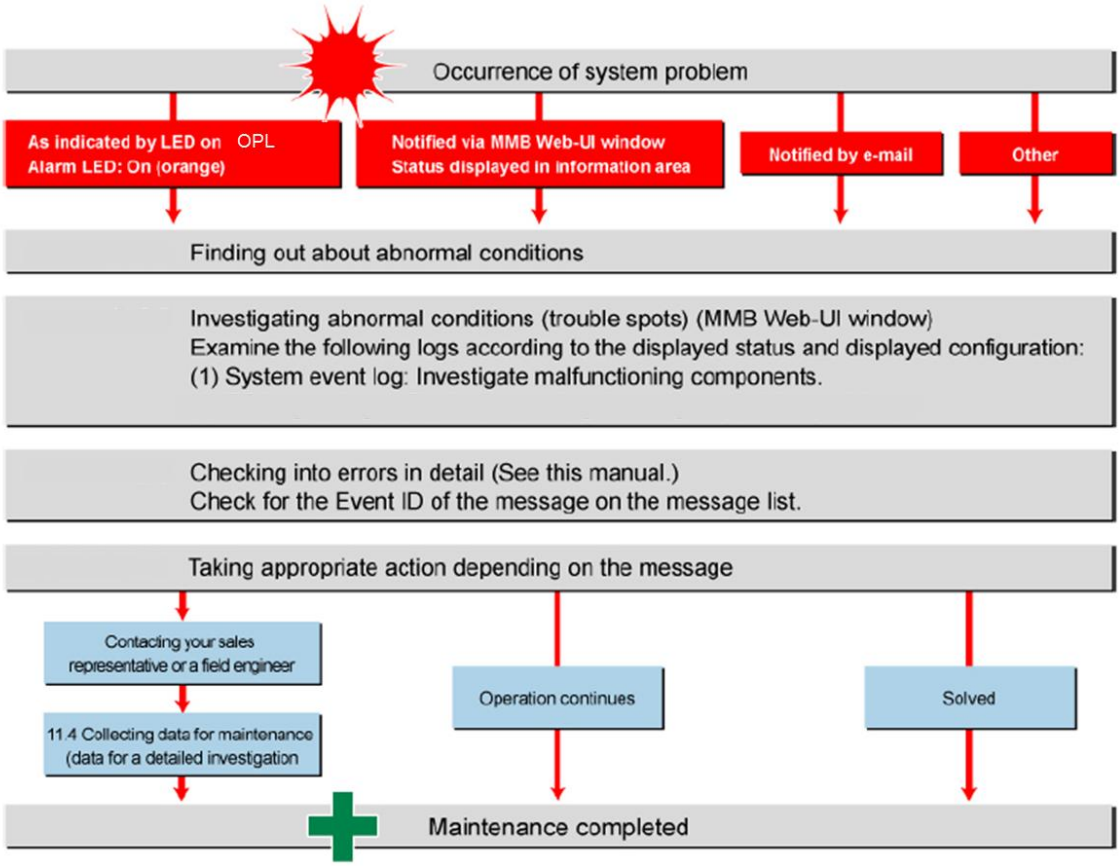
6.2 Troubleshooting

This section describes how to troubleshoot system problems.

6.2.1 Troubleshooting overview

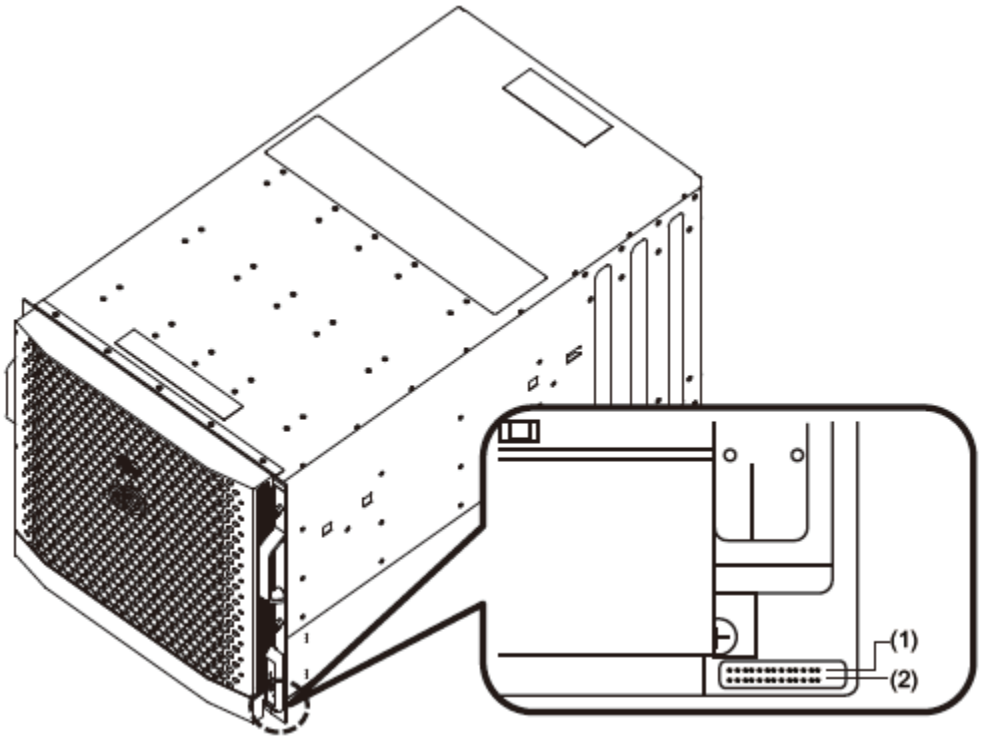
The following shows the basic procedure for troubleshooting.

FIGURE 6.1 Troubleshooting overview



If a problem occurs in this product, troubleshoot the problem according to the displayed message.
If the error recurs, contact your sales representative or a field engineer.
Before making contact, confirm the unit, source, part number, event ID, and description of the error as well as the model name and serial number shown on the label affixed to the main unit.

FIGURE 6.2 Label location



No.	Description
(1)	Model name
(2)	Serial number

6.2.2 Items to confirm before contacting a sales representative

Before contacting your sales representative, confirm the following details.
Print the sheet in Appendix G Failure Report Sheet, and enter the necessary information.

- Items to confirm
  Model name and type of the main unit.
  - You can confirm the model name and type with the MMB Web-UI. You can also confirm them from the label affixed to the main unit.
  - Hardware configuration (types and locations of the supplied built-in options)
  - Configuration information (BIOS setup utility settings)
  - OS used
  - LAN/WAN system configuration

Symptoms (e.g., what happened at the time, message displayed)
Sample messages:
System event log: See

- .
- Occurrence date and time
- Server installation environment
- Status of various lamps

6.2.3 Finding out about abnormal conditions

If a problem occurs in the system, use the LEDs on the front of the device, any report on the MMB Web-UI windows, and any e-mail notification to understand the situation. E-mail notification requires settings made in advance.

Remarks

If [Part Number] or [Serial Number] (the content or information area) in the MMB Web-UI window displays "Read Error," contact a field engineer or your sales representative.

Before making contact, confirm the model name and serial number shown on the label affixed to the main unit.

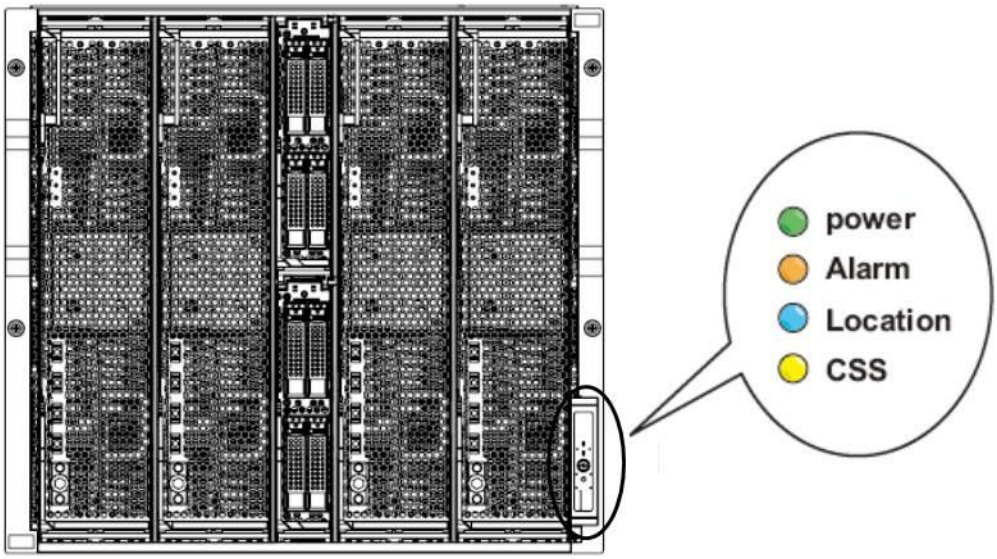
LED display

The following figure shows the LEDs located on the front panel of the device. The Alarm LED indicates a problem inside the device.

If a problem occurs inside the device, the Alarm LED goes on (orange).

The Alarm LED stays off when the device is operating normally.

FIGURE 6.3 Alarm LED on the front panel of the device



As long as a problem remains inside the device, the Alarm LED is on. This indication does not change even if multiple problems have occurred.

Note that the front panel of the device also has the MMB-Ready LED. The MMB-Ready LED stays on in green when the device is operating normally. To start the MMB, select [System] – [MMB] on the Web-UI when the MMB-Ready LED is off. Select [Enable] in [Enable/Disable MMB] in the [MMB] window. Then, click the [Apply] button.

MMB Web-UI window

The MMB Web-UI window always displays the information area. [Status] in the information area displays the system status. The following table lists the Normal, Warning, and Error status indicators. You can view the details of a message about a trouble spot by clicking the displayed icon to jump to the [System Event Log] window.

TABLE 6.3 Icons indicating the system status

Status	Display color	Icon	
Normal (normal status)	Green	None	
Warning (warning status)	Yellow		A black! Mark in a yellow triangle
Error (critical status)	Red		A white x mark in a red circle

Remarks
If [Part Number] or [Serial Number] (the content or information area) in the MMB Web-UI window displays "Read Error," contact a field engineer or your sales representative.
Before making contact, confirm the model name and serial number shown on the label affixed to the main unit.

Alarm E-Mail notification

Alarm E-Mail notification can inform you of system problems.
You can configure Alarm E-Mail notification for problem occurrences by selecting [Network Configuration] – [Alarm E-Mail] from the MMB menu.
You can also filter the notification, such as by error status type, or target component.

Miscellaneous

Problems related to system startup or drivers may occur.
If the status is one of the MMB error or warning statuses listed in the following operation interrupt criteria, stop the system and contact a field engineer or your sales representative.
Before making contact, confirm the model name and serial number shown on the label affixed to the main unit.

- Operation interrupt criteria
  - The Alarm LED of the MMB is on.
  - The Active LED of MMB is off.
  - You cannot connect to the MMB Web-UI.
  - The Alarm LEDs of multiple boards in the device are on.
  - The MMB Web-UI displays [Read Error].
  - The [System Status] window of the MMB Web-UI displays [Not Present] for the status of every unit.

6.2.4 Investigating abnormal conditions

Investigate trouble spots. First, check the component (e.g., SB, IOU) where the problem occurred.
The corrective action varies depending on various factors, including the location of the trouble spot, error level, and the system operation mode.

Finding out about a faulty component

Investigate the entire system component configuration and the faulty component.
Select [System] – [System Status] in the [MMB] menu window to display the window shown in the following figure.
You can find out the status of each component.
Click the icon displayed for an existing trouble spot to display a window showing the component status. If [Part Number] or [Serial Number] (the content or information area) in the MMB Web-UI window displays "Read Error," contact a field engineer or your sales representative.
You can view the component status and system event log (SEL) contents by selecting [System] – [System Event Log] to open the [System Event Log] window.
The SEL information is important for an investigation, so first click the [Download] button at the bottom of the window to save the information. The information will be needed when you contact a field engineer or your sales representative.

6.3 Notes on Troubleshooting

This section provides notes on troubleshooting.

- In the Cisco C880 server, if you unplug all the AC power cables while the device is in standby mode, the system event log records AC Lost (Severity: Info). This is neither a problem nor a failure. It is a normal situation.
  The following example shows this type of message.

(Item): Severity Unit Source EventID Description
--------- : ----------
(Display): Info PSU#*** ******** Power Supply input lost during the cabinet power off

6.4 Configuring and Checking Log Information

This section describes how to configure and confirm the log information on problems that occurred in the system.

6.4.1 List of log information

This section lists the types of log information that can be acquired.

- Available log information
- System event log
- Syslog and event log
- Hardware error log
- BIOS error log
- Information on factors in system power supply control
- Network configuration log information
- NTP client log information
- Operation log information
- Physical inventory information
- System configuration information
- System configuration file
- Information on internal rack sensor definitions

6.5 Firmware Updates

The Cisco C880 server is configured with BIOS, BMC, and MMB firmware.
Each firmware is managed as a total version integrating different versions.
The firmware is updated from the MMB in batch (applying to all the firmware at all locations within the system).

6.5.1 Notes on updating firmware

If the MMB or SB fails, perform maintenance on it before updating the firmware. Do not update the firmware in a configuration containing a faulty MMB or SB.
Firmware update can be performed regardless of power status of the system.
If the system is not power off, new firmware is applied after power off of the system.
Note
If the firmware update fails, update the firmware again by ‘Firmware Update’ menu of MMB Web-UI.

Appendix A Functions Provided by the Cisco C880 server

This appendix lists the functions provided by the Cisco C880 server. It also lists management network specifications.

A.1 Function List

The following lists the functions provided by the Cisco C880 server.

A.1.1 Action

TABLE A.1 Action

Operation	Minor item	Description
User operation	User operation setting	Operation privilege setting for each user account
	GUI	Web user interface
	CLI	MMB command line interface
External interface	KVM (local)	Local VGA, USB
Remote console	Console redirection	Serial console over LAN
	Video redirection	Function that uses PC connected to management LAN as graphical console
	Virtual media	Function that regards a drive in PC connecting via management LAN as the drive in the system.
UEFI	UEFI interface	UEFI shell
		Boot Manager

A.1.2 Operation

TABLE A.2 Operations

operation	Minor item	Description
System construction	Management LAN setting	MMB management LAN setting
		Maintenance LAN (CE port) setting
		Network setting internal LAN
	Operating privilege/range setting	User account management
	Memory Operation Mode	- Performance Mode - Normal Mode - Partial Memory Mirror Mode - Full Mirror Mode - Spare Mode
	Virtualization	MAC address fixing of internal LAN PCH
System operation/ power control	Start	Power-on by Web-UI, CLI or Wake On LAN
	Stop	Shutdown or forced power-off from Web-UI, CLI or OS
	Restart	Reboot from Web-UI or OS, system reset
	Power recovery processing	Power-on control when power is restored from AC Lost
	Boot control	Boot device selection in Web-UI
		Diagnosis mode selection at boot

operation	Minor item	Description
		Boot device selection by UEFI Boot Manager, boot option setting
	Scheduled operation	Automatic power-on/off at specified date and time specification
	Wake On LAN	Power-on via network
Automatic recovery	Degraded operation	Automatic degraded operation on CPU, DIMM, SB etc
	Reserved SB	SB automatic switching from faulty SB to Reserved SB
	ASR	Automatic restart of system when failure occurs
Continuous operation	Continuous operation	Recovery by MMB or BMC reset, continuous system operation
Ecological operation	Power consumption management	Cabinet power consumption monitoring, notification to higher-level software
	PSU power-on count control	PSU power-on control only as needed
	FAN speed control	Optimum control of FAN speed
Time synchronization	NTP client	NTP client

A.1.3 Monitoring and reporting functions

TABLE A.3 Monitoring and reporting functions

operation	Minor item	Description
Hardware monitoring and reporting	Hardware problem monitoring	Hardware problem monitoring by MMB/BMC/UEFI
	System problem monitoring	Watchdog Timer monitoring by MMB/UEFI
	Power control problem monitoring	Power control sequence problem monitoring
	FAN speed problem monitoring	Fan speed problem monitoring
	Voltage problem monitoring	Voltage problem monitoring
	Temperature problem monitoring	Temperature problem monitoring
	Hardware proactive monitoring	Proactive monitoring of CPU, DIMM, and HDD hardware failures
	External reporting	External reporting by e-mail, SNMP
	Event monitoring	Sensor-detected event monitoring
	Threshold monitoring	Threshold monitoring of temperature, power voltage, and fan speed
Status display	LED display	Display of MMB and system status
		Location display (Location LED)
		Faulty component display
	Eco-related status display	Cabinet power consumption display
		FAN speed display
		PSU/DDC power-on status display
		Temperature display
		Eco status acquisition from higher-level software (SNMP)

operation	Minor item	Description
Log	Log type	Expand contents and enhance history information of MMB-collected log - System event log - Hardware and UEFI error log - Power control and factor information - Network setting and log - MMB operation log, login record - Firmware version - Mounting unit information - Sensor information - Various firmware log dumps
	Log download	Batch download of MMB-collected logs (SEL download)
Hardware error processing	Fault location	Faulty component indication
	WHEA support	Support of Windows Hardware Error Architecture

A.1.4 Maintenance

TABLE A.4 Maintenance functions

operation	Minor item	Description
Component replacement	Replacement target	Cold replacement, non-hot/hot-system/hot maintenance
		Hot maintenance support by the hot plug
	Replacement target component indication	Replacement target component indicated by SEL or LED
FRU management	FRU management	FRU information management for FRU management target components Serial No., part No., product name, etc.
		System information management and backup by FRU
Log management	Log collection	Log collection and generation management by MMB
	Log clear	MMB log clear
Firmware management	Generation management	Management at one generation
	Version display	Overall version display
	Firmware update	Batch firmware update in Web-UI/CLI
		Version matching between SBs by MMB (BIOS/BMC)
		SB version confirmation at power-off
Configuration setting information management	Configuration setting information save and restore	Save and restoration of MMB/UEFI information
Maintenance guidance	Maintenance wizard	Component replacement procedure instructions on Web-UI
Failure cause search	Internal log trace	MMB/BMC internal log acquisition
	Dump function	MMB core dump
		sadump
	Hardware log	CPU/chip set hardware log

A.1.5 Redundancy functions

TABLE A.5 Redundancy functions

operation	Minor item	Description
Network	Management LAN duplication	Management LAN duplication switching
Power supply	Dual power feed	Dual power feed monitoring
	PSU redundancy	PSU N+1 redundancy monitoring and control

operation	Minor item	Description
Unit	FAN redundancy	Fan redundancy monitoring and control
Component and module	DIMM duplication	Memory Mirror mode
	DINN spare	Memory Spare Mode
	Firmware storing memory duplication	FWH duplication
System clock	Clock multiplexing	Cisco C880 server has oscillator on each SB.

A.1.6 External linkage functions

TABLE A.6 External linkage functions

operation	Minor item	Description
External IF/API	IPMI/RMCP	IPMI/RMCP interface
	SNMP	SNMP interface
	telnet/ssh	Access to MMB CLI via telnet/ssh
	http/https	Access to MMB Web-UI via http/https
	NTP	Time synchronization with NTP client of MMB
EMS linkage	Other management software linkage	Linkage with server management software of each company
UPS linkage	Power failure control	Coordinated support with UPS device in power failure shutdown processing
		User script execution support before power failure shuts down
External file device linkage	Increase file device	Support of increase file device

A.1.7 Security functions

TABLE A.7 Security functions

operation	Minor item	Description
Security setting	External IF security setting	Network security setting (SSL, SSH, etc.)
User management/ authentication	User authentication	MMB login account management
Audit trail	Operating log	Records such as MMB operating log and login history, etc.
TPM	TPM	Support of TPM function

A.2 Correspondence between Functions and Interfaces

The following shows the correspondence between the functions provided by Cisco C880 server and interfaces.

A.2.1 System information display

TABLE A.8 System information display

Function	MMB Web-UI	MMB CLI	UEFI
System status display (Error, Warning)	Supported		
System event log (SEL) display	Supported		
System event log (SEL) download	Supported		
MMB Web-UI/CLI operating log display	Supported		
System information display	Supported		

Function	MMB Web-UI	MMB CLI	UEFI
(P/N, S/ N)			
Firmware version display	Supported	Supported	

A.2.2 System settings

TABLE A.9 System settings

Function	MMB Web-UI	MMB CLI	UEFI
Primary and secondary power feed	Supported	Supported	
Power-on setting at power recovery	Supported	Supported	
Start delay time at power recovery	Supported	Supported	
Installation altitude	Supported	Supported	
PSU redundancy setting	Supported	Supported	
Effective and invalid setting of Power Saving function as the entire System	Supported		
Power consumption threshold (Limit value) setting of the entire System	Supported		

A.2.3 System operation

TABLE A.10 System operation

Function	MMB Web-UI	MMB CLI	UEFI
System power control (On/Off/Force P-off)	Supported	Supported	

A.2.4 Hardware status display

TABLE A.11 Hardware status display

Function	MMB Web-UI	MMB CLI	UEFI
LED status display	Supported		
LED operation (on, clear, blinking)	Supported		
PSU (power supply unit) power-on count and status display	Supported		
System power consumption display	Supported		
FAN status monitoring and FAN speed display	Supported		
Temperature monitoring and display	Supported		
Voltage monitoring and display	Supported		
SB status display (CPU, DIMM, Mezzanine, Chipset, TPM, BMC, clock)	Supported		
IOU status display	Supported		
DU status display	Supported		
OPL status display	Supported		
MMB status display	Supported		

A.2.5 Display of system configuration information

TABLE A.12 Display of system configuration information

Function	MMB Web-UI	MMB CLI	UEFI
System status display (number of CPUs, COREs, memory size, power status)	Supported		

A.2.6 System configuration and operation setting

TABLE A.13 System configuration and operation setting

Function	MMB Web-UI	MMB CLI	UEFI
CPU setting			Supported
ASR (Automatic Server Restart) setting	Supported		
I/O space allocation to I/O device			Supported
Memory Operation Mode	Supported	Supported	
Memory Mirror RAS Mode	Supported	Supported	
TPM			Supported

A.2.7 System operation

TABLE A.14 System operation

Function	MMB Web-UI	MMB CLI	UEFI
Video redirection/ Virtual media	Supported		
Console redirection		Supported	
UEFI shell			Supported

A.2.8 System power control

TABLE A.15 System power control

Function	MMB Web-UI	MMB CLI	UEFI
Power-on	Supported	Supported	
Power-off (shutdown)	Supported	Supported	
Reset	Supported	Supported	
NMI	Supported	Supported	
Forced power-off	Supported	Supported	
Diagnosis mode selection at power on	Supported		
Scheduled operation	Supported		

A.2.9 OS boot settings

TABLE A.16 OS boot settings

Function	MMB Web-UI	MMB CLI	UEFI
OS boot device selection			Supported
OS boot priority setting			Supported
OS boot option setting			Supported
OS boot delay time setting			Supported
PXE/iSCSI boot network device setting			Supported
Boot control (boot setting override)	Supported		

A.2.10 MMB user account control

TABLE A.17 MMB user account control

Function	MMB Web-UI	MMB CLI	UEFI
MMB user account setting and Display	Supported	Supported	
MMB login user display	Supported	Supported	

A.2.11 Server management network settings

TABLE A.18 Server management network settings

Function	MMB Web-UI	MMB CLI	UEFI
Setting of MMB date, time, and time zone	Supported	Supported	
MMB time synchronization (NTP) setting	Supported		
MMB management LAN setting	Supported	Supported	
Internal LAN setting	Supported		
Maintenance LAN setting	Supported	Supported	
MMB LAN port setting	Supported		
MMB network protocol setting	Supported	Supported	
SNMP setting	Supported	Supported	
SNMP setting (V3)	Supported		
SSL setting	Supported		
SSH setting	Supported	Supported	
Remote Server Management user setting (RMCP)	Supported		
Access control setting	Supported		
Alarm E-Mail setting	Supported		
MMB network status display command		Supported	

A.2.12 Maintenance

TABLE A.19 Maintenance

Function	MMB Web-UI	MMB CLI	UEFI
Batch firmware update	Supported	Supported	
MMB configuration information save and restore	Supported		
BIOS configuration information save and restore	Supported		
Maintenance wizard: Component Replacement	Supported		
Maintenance wizard: Maintenance mode setting and cancellation	Supported		

A.3 Management Network Specifications

The following lists the management network specifications of the Cisco C880 server.

TABLE A.20 Management network specifications

Component (A)	Communication direction	Component (B)	USER port	CE port	Protocol (Port No.)	Port No.
Terminal software	Duplex	(MMB)	Used	Used	telnet (TCP23)	Changeable
	Duplex				ssh (TCP 22)	Changeable
Video Redirection/ Virtual media	Duplex	MMB/ BMC	Used	Used	VNC (TCP80)	
FE terminal	Duplex	MMB	Used	Used	telnet (TCP23)	Changeable
	Duplex				ssh (TCP 22)	Changeable

Component (A)	Communication direction	Component (B)	USER port	CE port	Protocol (Port No.)	Port No.
	Duplex				RMCP (UDP623)	
NTP server (clock device)	Duplex	MMB (client)	Used	Used	NTP (UDP123)	
Web browser	Duplex	MMB	Used	Used	http/https (TCP 8081)	Changeable

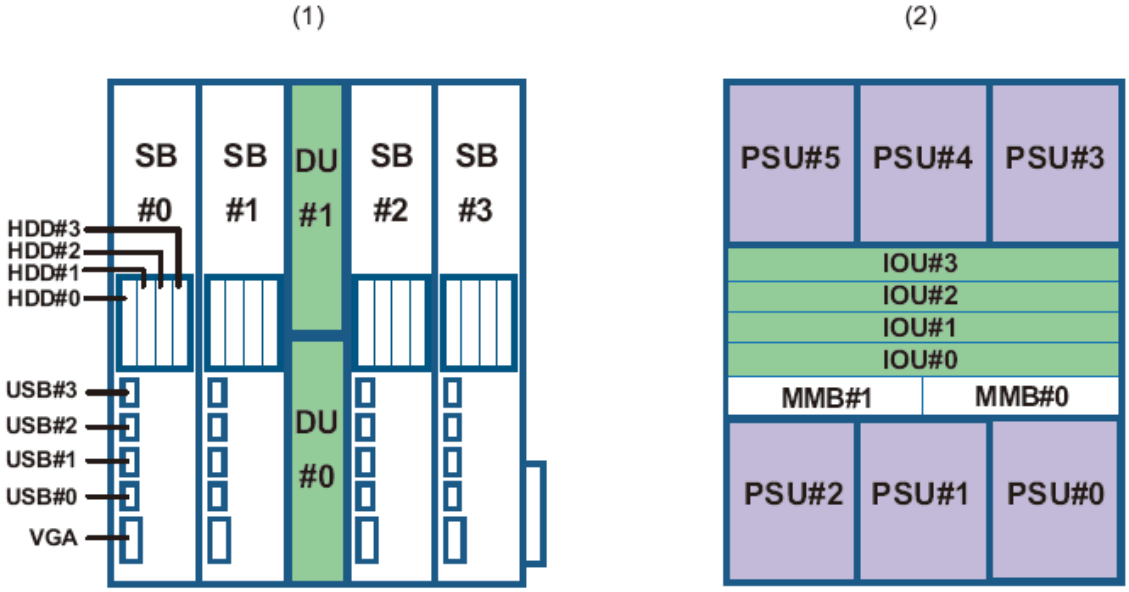
Appendix B Physical Mounting Locations and Port Numbers

This appendix describes the physical mounting locations of components, and shows MMB and IOU port numbers.

B.1 Physical Mounting Locations of Components

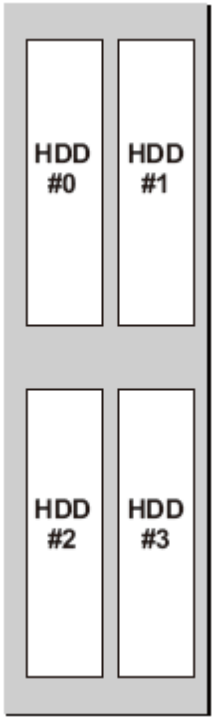
This section describes the physical mounting locations of components.

FIGURE B.1 Physical mounting locations in the Cisco C880 server



No.	Explanation
(1)	Front
(2)	Rear

FIGURE B.2 Physical mounting locations in the DU



B.2 Port Numbers

This section shows the numbering policy of each MMB and IOU port.

Remarks

The character strings used in numbering are the port numbers as viewed from firmware. These port numbers differ from the character strings in the port identification printed, stamped, or otherwise marked on units. FIGURE B.3 MMB port numbers shows MMB port numbering. “FIGURE B.7 IOU_1GbE port numbers” and “FIGURE B.8 IOU_10GbE port numbers” shows MMB port numbering.

FIGURE B.3 MMB port numbers

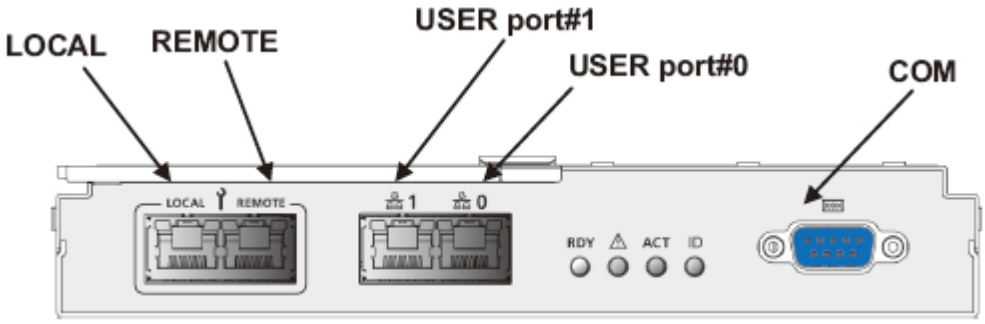


FIGURE B.4 IOU_1GbE port numbers

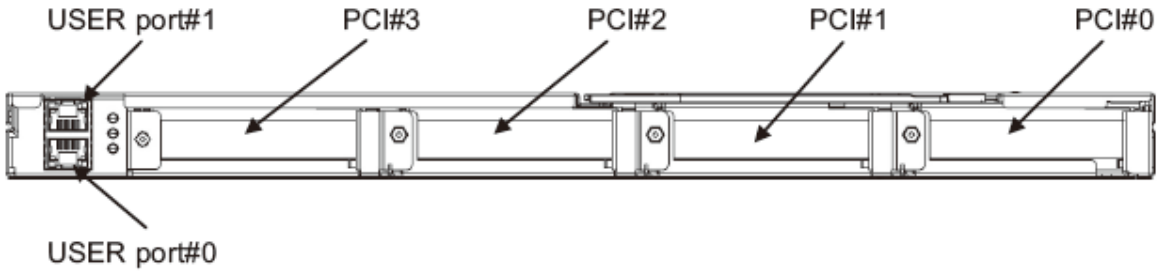
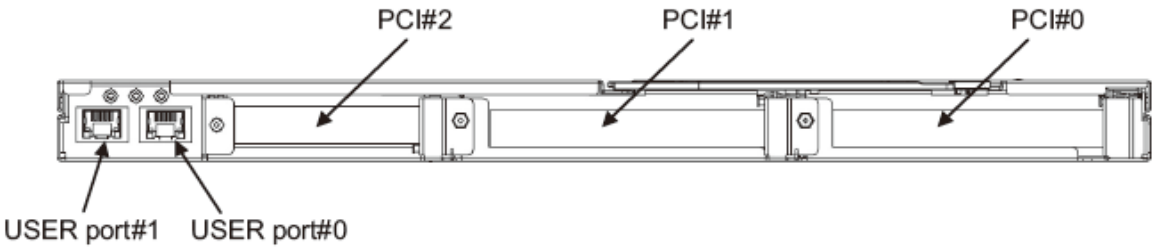


FIGURE B.5 IOU_10GbE port numbers



Appendix C Lists of External Interfaces Physical

This appendix describes the external interfaces of the Cisco C880 server.

C.1 List of External System Interfaces

The following lists the external system interfaces.

TABLE C.1 External system interfaces

IO interface	Mounting component	Number of ports	Location	Remarks
USB	SB	4	Front	USB 2.0
VGA	SB	1	Front	Max.1600 x 1200 dots, 65536 colors
LAN (IOU)	IOU_1GbE	2	Rear	GbE
	IOU_10GbE	2	Rear	10GbE
HDD/SSD	DU	4	Front	2.5inch HDD/SSD

C.2 List of External MMB Interfaces

The following lists the external MMB interfaces.

TABLE C.2 External MMB interfaces

External interface		Number of ports	Location	Remarks
LAN (MMB)	1000Base-T	2	Rear	User Port(Management LAN)
	100Base-TX	1	Rear	Maintenance LAN Port
COM		1	Rear	Connector Type: Dsub 9pin

Appendix D Physical Locations and BUS Numbers of Built-in I/O, and PCI Slot Mounting Locations and Slot Numbers

This appendix shows the correspondence between the physical locations and BUS numbers of built-in I/O in the Cisco C880 server. It also shows the correspondence between PCI slot mounting locations and slot numbers.

D.1 Physical Locations and BUS Numbers of Internal I/O Controllers of the Cisco C880 server

The following table shows physical location and BUS numbers of SB internal I/O controllers.
.

TABLE D.1 physical locations of SB internal I/O controllers and BUS numbers

Internal I/O	BUS:DEV:FUNC	Remarks
Home SB-USB EHCI controller	00:1A:0	USB Port #0
		USB Port #1
	00:1D:0	USB Port #2
		USB Port #3
		Video redirection
		Virtual media

D.2 Correspondence between PCI Slot Mounting Locations and Slot Numbers

The following table shows the correspondence between PCI slot mounting locations and slot numbers.

TABLE D.2 Correspondence between PCI Slot Mounting Locations and Slot Numbers

Mounting location		Slot number (decimal number)
Board	Slot	
SB#0	Port to IOU#0	4097
	Port to IOU#1	4098
	Port to IOU#2	4099
	Port to IOU#3	4100
SB#1	Port to IOU#0	4113
	Port to IOU#1	4114
	Port to IOU#2	4115
	Port to IOU#3	4116
SB#2	Port to IOU#0	4129
	Port to IOU#1	4130
	Port to IOU#2	4131

Mounting location		Slot number (decimal number)
Board	Slot	
	Port to IOU#3	4132
SB#3	Port to IOU#0	4145
	Port to IOU#1	4146
	Port to IOU#2	4147
	Port to IOU#3	4148
IOU#0	PCIC#0	2
	PCIC#1	3
	PCIC#2	4
	PCIC#3 (*1)	5
IOU#1	PCIC#0	18
	PCIC#1	19
	PCIC#2	20
	PCIC#3 (*1)	21
IOU#2	PCIC#0	34
	PCIC#1	35
	PCIC#2	36
	PCIC#3 (*1)	37
IOU#3	PCIC#0	50
	PCIC#1	51
	PCIC#2	52
	PCIC#3 (*1)	53

N/A: Not applicable
*1: IOU_10GbE does not have PCI Slot #3.

Appendix E Status Checks with LEDs

This appendix describes the types of mounted LEDs for the Cisco C880 server. It also describes how to check the status with LEDs.

E.1. LED Type

The Cisco C880 server has Customer Self Service (CSS) LED, System Alarm LED, and Location LED on front side of the cabinet. CSS LED and System Alarm LED indicate faulty status of entire system. Location LED indicates physical location of the system.
The Cisco C880 server also has Power LED, Alarm LED, and Location LED in components.
Power LED indicates power status in the component. Alarm LED indicates whether there is an error in the component. Location LED indicates the mounting location of the component. Location LED can be set to on and off. When you replace the component by using Maintenance Wizard, Location LED helps your work.

E.1.1 Power LED, Alarm LED, and Location LED

In principle, each component for the Cisco C880 server comes equipped with the following LEDs.

TABLE E.1 Power LED, Alarm LED, and Location LED

LED type	Color	Function
Power	Green	Indicates the power status of the component.
Alarm	Orange	Indicates whether there is an error in the component.
Location	Blue	- Identifies the component (location). - Can be arbitrarily set to blink or turned off by the user. - Indicates the component undergoing maintenance when Maintenance Wizard is running.

E.1.2 PSU

The PSU comes equipped with the following LED.

TABLE E.2 PSU LED

LED type	Color	Function
FANM#0 Alarm	Orange	Indicates state of FANM#0.
Power/Alarm	Yellow/Green	Indicates whether there is AC input to each PSU, whether there is an error in the PSU, and the PSU on/off status.
FANM#1 Alarm	Orange	Indicates state of FANM#1

TABLE E.3 Power status and PSU LED display

Status	FANM#0 Alarm	Power/Alarm	FANM#1 Alarm	OPL CSS (*2)
PSU AC input is off.	Off	Off	Off	Off
AC input is on, and the PSU is off.	Off	Blinking in green	Off	Off
AC input is on, and the PSU is on.	Off	On (green)	Off	Off
PSU temperature error is predicted.	Off	On (green)	Off	On (yellow)
PSU temperature error is detected or the power system error in a PSU is predicted.	Off	Blinking in green	Off	On (yellow)
The power system of a PSU failed.	Off	On (yellow)	Off	On (yellow)
FANM#0 error occurs	Off or On (Orange) (*1)	Off	Off	On (yellow)
FANM#1 error occurs	Off	Off	Off or On (Orange) (*1)	On (yellow)

(*1) If Alarm LED is turning on orange, the FANM with the particular LED fails. Even though Alarm LED remains off, SEL may be displayed which indicates the FANM error due to detecting not enough fan rotation by preventive fan monitoring function.

(*2) There is a CSS LED on an OPL, not a PSU.

E.1.3 FANU

The FANU comes equipped with the following LED.

TABLE E.4 FAN LED

LED type	Color	Function
FANM#0 Alarm	Orange	Indicates state of FANM#0.
Power/Alarm	Green	Indicates power state of PSU supplying power to FANU.
FANM#1 Alarm	Orange	Indicates state of FANM#1

TABLE E.5 Power status and FANU LED display

Status	FANM#0 Alarm	Power/Alarm	FANM#1 Alarm	OPL CSS (*2)
PSU AC input is off.	Off	Off	Off	Off
AC input is on, and the PSU is off.	Off	Blinking in green	Off	Off
AC input is on, and the PSU is on.	Off	On (green)	Off	Off
FANU temperature error is predicted.	Off	On (green)	Off	On (yellow)
FANU temperature error is detected or the power system error in a PSU is predicted.	Off	Blinking in green	Off	On (yellow)
The power system of a FANU failed.	Off	On (yellow)	Off	On (yellow)
FANM#0 error occurs	Off or On (Orange) (*1)	Off	Off	On (yellow)
FANM#1 error occurs	Off	Off	Off or On (Orange) (*1)	On (yellow)

(*1) If Alarm LED is turning on orange, the FANM with the particular LED fails. Even though Alarm LED remains off, SEL may be displayed which indicates the FANM error due to detecting not enough fan rotation by preventive fan monitoring function.

(*2) There is a CSS LED on an OPL, not a PSU.

E.1.4 SB

SB comes equipped with the following LED.

TABLE E.6 SB LED

LED type	Color	Function
Power	Green	Indicates power state in a SB.
Alarm	Orange	Indicates whether there is error or not in a SB.
Location	Blue	Specifies a SB. - Can be arbitrarily set to blink or turned off by the user. - Indicates the component undergoing maintenance when Maintenance Wizard is running.

TABLE E.7 SB status and SB LED display

Status	Power	Alarm	Location
AC off and system power Off	Off	Off	Off
System Power On	On (green)		
Error of SB		On (orange)	
Identifying SB (Turn on by Maintenance Wizard)			On (blue)

E.1.5 IOU

IOU which is IOU_1GbE or IOU_10GbE comes equipped with the following LED.

TABLE E.8 IOU LED

LED type	Color	Function
Power	Green	Indicates power state in an IOU.
Alarm	Orange	Indicates whether there is error or not in an IOU.
Location	Blue	Specifies an IOU. - Can be arbitrarily set to blink or turned off by the user.

LED type	Color	Function
		- Indicates the component undergoing maintenance when Maintenance Wizard is running.

TABLE E.9 IOU status and IOU LED display

Status	Power	Alarm	Location
AC off and system power Off	Off	Off	Off
System Power On	On (green)		
Error of IOU		On (orange)	
Identifying IOU (Turn on by Maintenance Wizard)			On (blue)

E.1.6 PCI Express slot of IOU

There is no LED in PCI Express slots of IOU.
To mount and unmounts PCI Express card in an IOU physically, take off the IOU from a cabinet.

E.1.7 DU

DU comes equipped with the following LED. Only Power LED is used. Attention LED is not used.

TABLE E.10 DU LED

LED type	Color	Function
Power Left	Green	Indicates power state in a DU.
Alarm Right	Green	Indicates power state in a DU.
Attention Left	Orange	Not used.
Attention Right	Orange	Not used.

TABLE E.11 DU status and DU LED display

Status	Power Left	Power Right	Attention Left	Attention Right
System including PCI Express slot #0 On	On (green)		Off	Off
System including PCI Express slot #1 On		On (green)	Off	Off

E.1.8 HDD/SSD

The HDD or SSD comes equipped with the following LEDs.

TABLE E.12 HDD/SSD LED

LED type	Color	Function	Note
HDD/SSD Access	Green	Indicates the HDD or SSD access status.	Mounted in only HDD or SSD.
HDD/SSD Alarm	Orange	Indicates whether there is an error in the HDD or SSD and the hot operation status.	Mounted in only HDD or SSD.

TABLE E.13 HDD/SSD status and LED display

HDD/SSD status	HDD/SSD Access	HDD/SSD Alarm	Note
Accessing to HDD or SSD	Blinking	Off	
Error of HDD or SSD	Off	On	When RAID configuration breaks. When Agent is offline.
Indicating location of HDD or SSD	Off	Blinking periodically with 3 Hz	When using SAS RAID card.
Rebuilding array	Blinking	Blinking periodically with 1 Hz	When using SAS RAID card.

E.1.9 MMB

The MMB comes equipped with the Active LED, Ready LED and Location LED. The Active LED indicates the active MMB, and the Ready LED indicates the MMB firmware status. Location LED is used to specify the MMB.
After the MMB firmware starts, the active MMB turns on the Active LED. The Ready LED blinks while MMB firmware startup is in progress. The Ready LED stays on when the startup is completed.

TABLE E.14 MMB LED

LED type	Color	Function
Ready	Green	Indicates the MMB status.
Alarm	Orange	Indicates whether there is an error in the MMB.
Active	Green	Indicates whether the MMB is the active or standby MMB.
Location (ID)	Blue	Identifies the MMB.

TABLE E.15 MMB (device) status and LED display

MMB status/device status	Ready	Alarm	Active	Location
MMB startup is in progress.	Blinking			
The MMB has started normally (Ready status).	On			
An error occurred in the MMB.		On		
The MMB is the standby MMB.			Off	
The MMB is the active MMB.			On	
The MMB is being located.				On

E.1.10 LAN

The LAN port comes equipped with the following LEDs. LAN ports in an IOU and LAN ports in a MMB have same LEDs.

TABLE E.16 LAN LEDs

LED type	Color	Function	Note
100M LAN Link/Act	Green	Indicates the Link status and Activity status of a 100M LAN.	Mounted only on the MMB
100M LAN Speed	Green	Indicates the communication speed of a 100M LAN.	Mounted only on the MMB
GbE LAN Link/Act (*1)	Green	Indicates the Link status and Activity status of a GbE LAN.	Mounted only on the IOU_1GbE
GbE LAN Speed (*1)	Green/Orange	Indicates the communication speed of a GbE LAN.	Mounted only on the IOU_1GbE
10GbE LAN Link/Act (*1)	Green	Indicates the Link status and Activity status of a 10GbE LAN.	Mounted only on the IOU_10GbE
10GbE LAN Speed (*1)	Green/Orange	Indicates the communication speed of a 10GbE LAN.	Mounted only on the IOU_10GbE

(*1) It is not enough to confirm the ‘Link’ state by only checking that Link LED is turning on. You can confirm that the LAN port is Link ‘state’ by not only checking that Link LED is turning on but also checking that the particular LAN port is ‘Enabled’ by MMB Web-UI.

TABLE E.17 LAN LED and Linkup Speed

NIC	Speed			
	10M	100M	1G	10G
GbE	Off	Green	Yellow	-
10GbE	-	Off	Yellow	Green

E.1.11 OPL

The OPL comes equipped with an LED indicating the status of entire system, the MMB Ready LED, and the System Alarm LED. From the OPL LED display, you can check the power status of the entire device, check for any problem, and check the MMB firmware status.

TABLE E.18 OPL LED

LED type	Color	Function
System Power	Green	Indicates the power status of the system.
CSS	Yellow	
System Alarm	Orange	Indicates whether there is an error in the system.
System Location	Blue	Identifies the system. - Can be arbitrarily turned on, set to blink, or turned off by the user.

TABLE E.19 System status and LED display

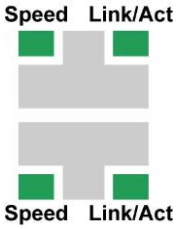
System status	System Power	CSS	System Alarm	Location
The system power status is standby. Standby status means that MMB is running and the system is off.	On (orange)			
System is on.	On (green)			
Warning or Error of CSS components in the system.		On		
Warning or Error of components other than CSS components in the system.			On	
Identifying the system.				On

E.2 LED Mounting Locations

This section describes the physical LED mounting locations on each component.

- Components equipped with Power, Alarm, and Location LEDs have the LEDs mounted as follows.
  - The order of mounted LEDs arranged from left to right is as follows: Power, Alarm, Location.
  - The order of mounted LEDs arranged from top to bottom is as follows: Power, Alarm, Location.
- From the standpoint of appearance, components equipped with LAN ports have the Speed LED on the left and the Link/Act LED on the right of each port.

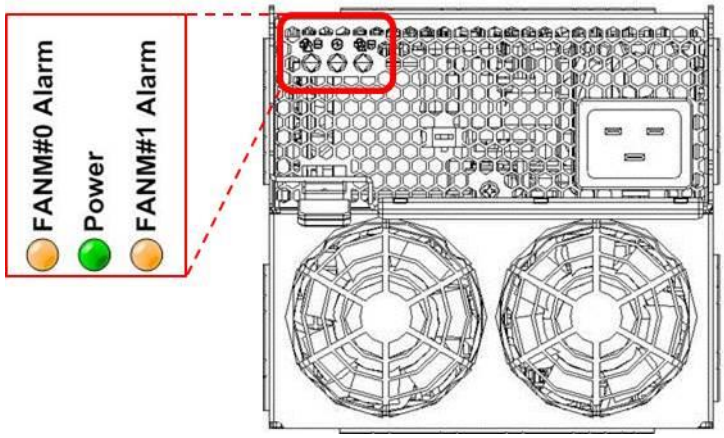
FIGURE E.1 LED mounting locations on components equipped with LAN ports



LEDs

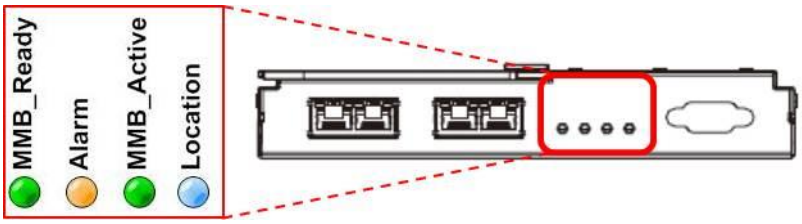
- The order of PSU and FANU LEDs arranged from the left or the top is as follows: FANM#0 Alarm, Power, and FANM#1 Alarm.

FIGURE E.2 Mounting locations of PSU and FANU



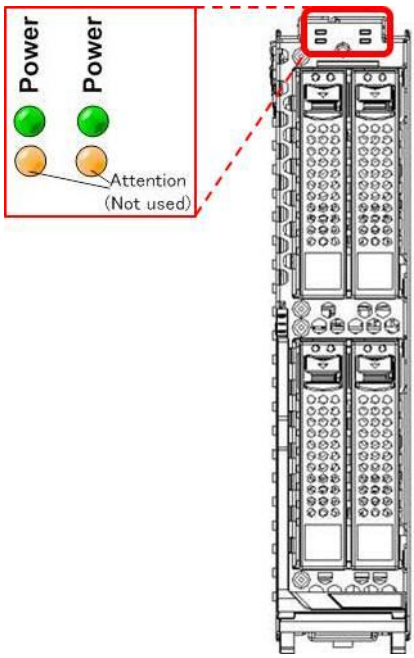
- The order of MMB LEDs arranged from the left or the top is as follows: Ready, Alarm, Active, and Location.

FIGURE E.3 MMB LED mounting locations



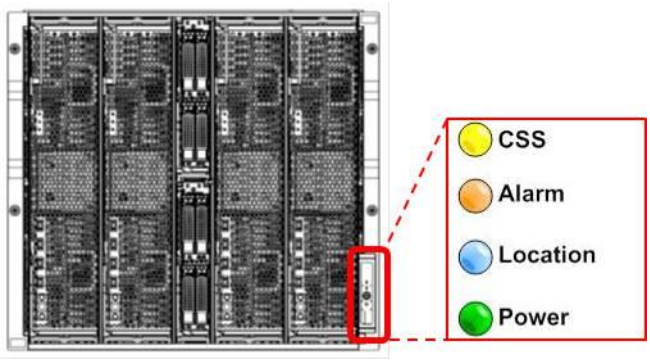
- The order of DU LEDs arranged as follows.

FIGURE E.4 DU LED mounting locations



- The order of System LEDs arranged from the left or the top is as follows: Power, Alarm, CSS, Location, MMB_Ready.

FIGURE E.5 System LED mounting locations



E.3 LED list

The following table lists the mounted LEDs for the Cisco C880 server.

TABLE E.20 LED list (1/3)

Component	LED type	Color	Quantity	Status	Description
PSU	Power/ Alarm	Green/ orange	1	Off	PSU AC input off
				Blinking in green	PSU AC input on and PSU off See also E.1.2 PSU.
				On (green)	PSU AC input on and PSU on See also E.1.2 PSU.
				On (yellow)	Error at PSU
	FANM#0 Alarm	Orange	1	Off	Normal status in FANM#0 See also E.1.2 PSU.
				On	Error at FANM#0
	FANM#1 Alarm	Orange	1	Off	Normal status in FANM#1
				On	Error at FANM#1 See also E.1.2 PSU.
FANU	Power/ Alarm	Green	1	Off	PSU AC input off or no DC output to FANM
				Blinking	PSU AC input on and PSU off See also E.1.3 FANU.
				On	PSU AC input on and any of PSU in system on See also E.1.3 FANU.
	FANM#0 Alarm	Orange	1	Off	Normal status in FANM#0 See also E.1.3 FANU.
				On	Error at FANM#0
	FANM#1 Alarm	Orange	1	Off	Normal status in FANM#1
				On	Error at FANM#1 See also E.1.3 FANU.
SB	Power	Green		Off	SB power off
				On	SB power on
	Alarm	Orange		Off	SB normal
				On	Error in SB
	Location	Blue		Off	
				On	Identify SB

TABLE E.21 LED list (2/3)

Component		LED type	Color	Quantity	Status		Description
IOU		Power	Green		Off		IOU power off
					On		IOU power on
		Alarm	Orange		Off		IOU normal
					On		Error in IOU
		Location	Blue		Off		
					On or Blinking		Component location
	LAN (IOU_1GbE)	Link/Act	Green		Off		Network not link
					Blinking in green		Network active
					On (green)		Network link
		Speed	Green/ Orange		Off		10Mbps
					On (green)		100Mbps
					On (orange)		1000Mbps
	LAN (IOU_10GbE)	Link/Act	Green		Off		Network not link
					Blinking in green		Network active
					On (green)		Network link
		Speed	Green/ Orange		Off		100Mbps
					On (green)		1000Mbps
					On (orange)		10Gbps
DU		Power	Green		Off		DU power off
					On		DU power on
		Attention	Orange		Off		
	HDD/SSD	Access	Green		Off		Non-active
					On		Active
		Alarm	Orange		Off		HDD/SSD normal
					On		Error in HDD/SSD
					Blinking	low speed (1Hz)	Rebuilding array in RAID
						High speed (3Hz)	Indicate location
MMB		Location	Blue		Off		
					On		Specify the MMB
		Ready	Green		Off		MMB not initialized
					Blinking		MMB initialization in progress
					On		MMB initialization complete (normal MMB operating status)
		Active	Green		Off		
					Blinking in green		Active MMB location
		Alarm	Orange		Off		
					On		Error in MMB
	LAN 100BASE-TX (MMB) (*1)	Link/Act	Green		Off		Network not link
					Blinking in green		Network active
					On (green)		Network link
		Speed	Green/ Orange		Off		10Mbps
					On		100Mbps

(*1) Since MMB does not close its LAN port explicitly, the state where LAN port is disabled is not displayed.

TABLE E.22 LED list (3/3)

Component	LED type	Color	Quantity	Status	Description
OPL	System Power	Green		Off	Power off in the system
				On	- Power on in the system - PSU on, 12V feed
	System Alarm	Orange		Off	
				On	Error occurrence in cabinet
	System Location (ID)	Blue		Off	
				On	Identify cabinet
	CSS	Yellow		Off	
				On	Error in CSS component

Appendix F Component Mounting Conditions

This appendix describes the mounting conditions of components for the Cisco C880 server.

F.1 CPU

This section describes the number of CPUs that can be mounted and the criteria for mixing different types of CPU.

CPU mounting criteria

- Two CPUs must be mounted in a SB.

CPU mixing condition

- In the system, all CPUs must have the same frequency, cache size, core number, power, QPI rate, and scale.

F.2 DIMM

This section describes the number of DIMMs that can be mounted and the criteria for mixing different types of DIMM.

DIMM mounting conditions

- At least two DIMMs are required per CPU.
- Up to 24 DIMMs can be mounted per CPU.
- DIMMs must be mounted in the following units:
  two DIMMs when normal mode, four DIMMs when full mirror mode or partial mirror mode, and six DIMMs when spare mode.

DIMM mixing criteria

DIMM criteria for Cisco C880 M4 server (E7-8800 v3 CPU).

- 16GB DIMMs and 32 GB DIMMs cannot be mixed in an SB or system.
- 32GB RDIMMs and 32 GB LRDIMMs cannot be mixed in an SB or system.

TABLE F.1 Relationship between DIMM size and mutual operability (within an SB)

DIMM size	16 GB RDIMM	32 GB RDIMM	32 GB LRDIMM
16 GB RDIMM	Supported	Not supported	Not supported
32 GB RDIMM	Not supported	Supported	Not supported
32 GB LRDIMM	Not supported	Not supported	Supported

TABLE F.2 Relationship between DIMM size and mutual operability (within the system)

DIMM size	16 GB	32 GB
16 GB	Supported	Not supported
32 GB	Not supported	Supported

DIMM criteria for Cisco C880 M4 server (E7-8800 v2 CPU).

- 16GB DIMMs and 32 GB DIMMs cannot be mixed in an SB or system.

TABLE F.3 Relationship between DIMM size and mutual operability (within an SB)

DIMM size	16 GB	32 GB
16 GB	Supported	Not supported
32 GB	Not supported	Supported

TABLE F.4 Relationship between DIMM size and mutual operability (within the system)

DIMM size	16 GB	32 GB
16 GB	Supported	Not supported
32 GB	Not supported	Supported

DIMM mounting order

The order of DIMM installation is shown below.

In below table, DIMMs are installed in order from one with small number.

TABLE F.5 DIMM mounting order in special case in SB

	CPU#0								CPU#1							
DIMM Slot#	0A0	0A3	0B0	0B3	0C0	0C3	0D0	0D3	1A0	1A3	1B0	1B3	1C0	1C3	1D0	0D3
	0A1	0A4	0B1	0B4	0C1	0C4	0D1	0D4	1A1	1A4	1B1	1B4	1C1	1C4	1D1	0D4
	0A2	0A5	0B2	0B5	0C2	0C5	0D2	0D5	1A2	1A5	1B2	1B5	1C2	1C5	1D2	0D5
Normal	1	1	4	4	2	2	6	6	1	1	5	5	3	3	7	7
	8	8	12	12	10	10	14	14	9	9	13	13	11	11	15	15
	16	16	20	20	18	18	22	22	17	17	21	21	19	19	23	23
Full or Partial Mirror	1	1	1	1	2	2	2	2	1	1	1	1	3	3	3	3
	4	4	4	4	6	6	6	6	5	5	5	5	7	7	7	7
	8	8	8	8	10	10	10	10	9	9	9	9	11	11	11	11
Spare	1	1	4	4	2	2	6	6	1	1	5	5	3	3	7	7
	1	1	4	4	2	2	6	6	1	1	5	5	3	3	7	7
	1	1	4	4	2	2	6	6	1	1	5	5	3	3	7	7

F.3 Available internal I/O ports

The following table lists the number of available internal I/O ports.

TABLE F.6 Available internal I/O ports and the quantities

Internal I/O		No.	Remarks
SB	USB	4	SB#0 only
	VGA	1	SB#0 only
IOU_1GbE	GbE	2	
IOU_10GbE	10GbE	2	
DU	HDD/SSD	4	

F.4 Legacy BIOS Compatibility (CSM)

The Cisco C880 server uses the UEFI, which is firmware that provides the BIOS emulation function. Currently, the following legacy BIOS restrictions are known:

- Option ROM area restriction: The number of PXE-enabled cards that can operate as boot devices is restricted to four.
- I/O space restriction: In a legacy BIOS environment, I/O space is required on a boot device.

Note
In a CSM environment, I/O space must be allocated to a boot device.

F.5 NIC (Network Interface Card)

Note the following precautions on mounting of a NIC (network interface card).
Notes

- We recommend specifying the members of teaming between LANs of the same type. (We recommend teaming between cards of the same type in the onboard LAN.)
- If the teaming is specified with different types of LAN, the scaling function on the receive side may be off because of differences in the scaling function.
  Consequently, the balance of receive traffic may not be optimized, but this is not a problem for normal operation.
- Depending on the Intel PROSet version used at the time of teaming configuration, a warning may be output about scaling on the receive side being disabled for the above-described reasons. In this event, simply click the [OK] button.
  For details on the scaling function on the receive side or other precautions, see the help for Intel PROSet

or check the information at [Device Manager] – [Properties *of the target LAN*] – [Details] – [Receive-Side Scaling].

- For the WOL (Wake on LAN) support conditions of operating systems, see the respective operating system manuals and restrictions. For remote power control in an operating system that does not support WOL, perform operations from the MMB Web-UI.

Appendix G Failure Report Sheet

This appendix includes the failure report sheet. Use this sheet to report a failure.

G.1 Failure Report Sheet

Model name	□ Cisco C880 server
OS	□ Red Hat Enterprise Linux (Version:) □ Windows Sever (Version:) □ Vmware (Version:)
Server installation environment	
LAN/WAN system configuration	
Hardware configuration	(Installed option types and locations)
Configuration information	(UEFI Setup Utility settings)
Occurrence date and time	Year Month Day Hour Minute
Frequency	□ Constantly □ Intermittently (times per) □ Unknown
Triggered by	Working before failure occurred? □ Yes □ No Current situation: Work details: Work affected? □ Yes □ No
Symptom	□ Hanging □ Slowdown □ Reboot □ OS panic/stop □ OS startup not possible □ Communication unavailable □ Other ( )
Error message	System event log: Agent log/Driver log: OS message: Other:
Status of various lamps	
Supplementary information	□ Yes □ No